Charter of Trust

Charter of Trust launches

Cyber Deterrence

in the private sector

Publication date: 30 June 2026

Charter of Trust – Cyber Deterrence Working Group

Classification: CoT Public

Cyber defense alone is no longer sufficient. While Charter of Trust continues to invest in detection and protection through its working groups on Security by Default, AI, PQC and Supply Chain cybersecurity, the economic logic of cybercrime remains intact: attacks are profitable, adversaries face little accountability, and the cost of attacking stays low.

What is missing is deterrence: raising the cost and risk for adversaries to the point where attacks become less attractive.

No single organization can achieve this alone. Collective action across industries, combined with structured intelligence sharing, rigorous testing of deterrence methods, and engagement with international institutions, is the only path to fundamentally shifting the dynamic.

The Charter of Trust equips itself with a new working group as the collaborative network of thought leaders, practitioners, testing groups, and solution providers driving cyber deterrence expertise in the private sector.

1. A New Cybersecurity Challenge: Defense Alone Is No Longer Enough

Cyber defense has come a long way. Organizations have invested heavily in firewalls, detection systems, and incident response capabilities. Yet despite this progress, the fundamental dynamic of the cyber threat landscape has not shifted in favor of defenders. Daily attacks have increased fourfold within the past year. Ransomware campaigns continue with little consequence for those responsible, despite some countries' bans on payments. State-backed actors operate for extended periods without being uncovered, incidents rising by more than 50% year over year since 2023. DDoS attacks disrupt critical services with near-total impunity. Lastly, the democratization of attack skills by AI has driven an 89% surge in AI-enabled attacks from 2024 to 2025.

The reason for this bleak landscape is structural: cybercrime remains economically rational. Less than 1% of organized cybercrime is estimated to be detected and prosecuted just in the US. As long as malicious activity is profitable and the risk of being held accountable is low, attackers retain strong incentives to continue. Detection has improved but detection alone does not deter. Cyber defenses, while essential, risk being overwhelmed by the sheer volume and velocity of AI-accelerated threats. A defensive posture addresses only one side of the equation. It reduces the impact of attacks but does not alter the underlying cost-benefit calculus for adversaries.

The geopolitical context amplifies this challenge further. State actors deliberately target critical infrastructure, including energy supply, healthcare systems, and government networks. Cyber incidents can quickly extend beyond a single company or country through deliberate or automated spread. Meanwhile, cross-jurisdiction cooperation remains complex, and the regulatory environment is fragmenting between offensive cyber and reactive measures.

Deterrence against cyber threats, compared to its traditional definition related to states' kinetic and nuclear power, is difficult to translate to the cyber realm for its diffuseness. National cyber deterrence postures are developing but lag behind because they remain insufficiently connected to the private sector, creating a gap between state-level deterrence and the organizations most frequently targeted.

What the current environment demands is a shift in thinking: from purely reactive defense to proactive deterrence. We need both: cyber defense and cyber deterrence.

2. The Charter of Trust Approach: Defeating the Cybercrime Business Model

The core logic of cyber deterrence is straightforward: make attacks riskier and more expensive for adversaries. Where cyber defense focuses on protecting one's own systems, cyber deterrence focuses on the adversary — on disrupting their operational model and altering their incentives.

A critical starting point is understanding how attackers work and how they choose their targets. Attackers conduct reconnaissance to identify and prioritize victims. If the methods and criteria by which targets are selected become transparent and better understood across the defender community, this knowledge itself becomes a deterrence mechanism — increasing attacker effort, reducing predictability of success, and raising operational cost. This approach can be understood as deterrence by obscurance: denying adversaries the informational advantage that makes their targeting efficient.

The CoT framework centers on two primary levers:

- **Cost:** Increasing the operational effort, time, and resources required to execute a successful attack. Time is among the highest costs an attacker faces. Disrupting reconnaissance, complicating attribution, and slowing lateral movement raises this cost directly. Resilient, self-recovering systems increase attacker fatigue. CoT will focus on identifying the factors that most effectively disrupt the economic viability of cybercrime.
- **Risk**: Increasing the probability of identification, exposure, and legal consequence. Collective attribution, structured intelligence sharing, and public transparency about adversaries all contribute to raising the risk adversaries face.

These two levers are CoT's strategic priorities. How exactly cost and risk are measured and benchmarked will be defined and refined over the course of the working group's activities. Every initiative CoT pursues will be evaluated against its contribution to raising adversary cost or risk.

Effective deterrence cannot be achieved in isolation. Several structural barriers must be overcome collectively: fragmented public-private cooperation, legal and jurisdictional complexity, uneven capabilities across the ecosystem, and AI-accelerated attack cycles that are already outpacing human-led response processes. No single organization can address these challenges alone — which is exactly why a cross-industry coalition is needed.

3. How CoT Advances Deterrence: Three Areas of Collective Action

The Charter of Trust operationalizes its deterrence approach through three interconnected focus areas.

Collective Attribution and Intelligence Sharing

CoT will establish a formalized mechanism for structured, real-time anonymized threat intelligence exchange among member organizations — moving beyond sporadic informal communication toward a shared operational cybersecurity capability. A centralized function will transform raw data into actionable intelligence, ensuring as a next step that smaller partners and supply chain participants can effectively consume and act on shared insights.

A flagship initiative in this area is Netwatch, a global cyber hunting capability. Through cryptographically secure and anonymized data sharing, Netwatch enables collective attribution of attacks and provides curated threat intelligence accessible in real-time. A pilot is planned for Q3 2026 among Charter of Trust members to test whether unified attribution measurably reduces attacker anonymity and deters operations. Increasing public transparency about attack sources and adversary methods is a core part of this effort to raise risk for attackers by reducing their anonymity.

Testing Cyber Deterrence

Cyber deterrence is an emerging concept and discipline. Defining what works requires active experimentation. CoT will systematically test and evaluate concrete deterrence methods against the cost and risk framework outlined above. This includes piloting approaches such as unified attribution to reduce attacker anonymity, publishing targeting methodologies used by threat actors to disrupt their reconnaissance advantage, and evaluating the impact of collective intelligence sharing on attacker behavior.

Engagement with Authorities and International Institutions

Effective deterrence ultimately requires a connection between private sector intelligence and the broader institutional landscape. CoT will consider cooperation with national and international authorities and institutions to ensure that private sector insights can inform and strengthen the cybercrime disruptive action frameworks being developed globally. The legal dimension, including the definition of boundaries for proportional political and law enforcement countermeasures, is an area where CoT actively will engage with policymakers.

4. Call to Action

The structural weaknesses in global cybersecurity cannot be solved in isolation. The CoT Cyber Deterrence Working Group offers a unique platform — cross-industry, cross-border, and connected to the governmental and international bodies shaping the future rules of engagement in cyberspace. As both target and technology provider, Charter of Trust members realize an obligation and an opportunity to validate deterrence methods empirically, not theoretically.

The goal is clear: collectively defeat the cybercrime business model, secure supply chains, and establish a new proactive standard for global digital trust.