AI-Resistant Cybersecurity Protection for Governments

The Operational Technology Challenge for Governments

Governments are responsible for keeping the critical infrastructure operational for their citizens, but they are also responsible for securing government-operated networks. In the US, published specifications like NIST 800-207 (Zero Trust Architecture), CISA's Zero Trust Maturity Model 2.0, and the DoD Zero Trust Reference Architecture have helped government enterprises build secure networks.

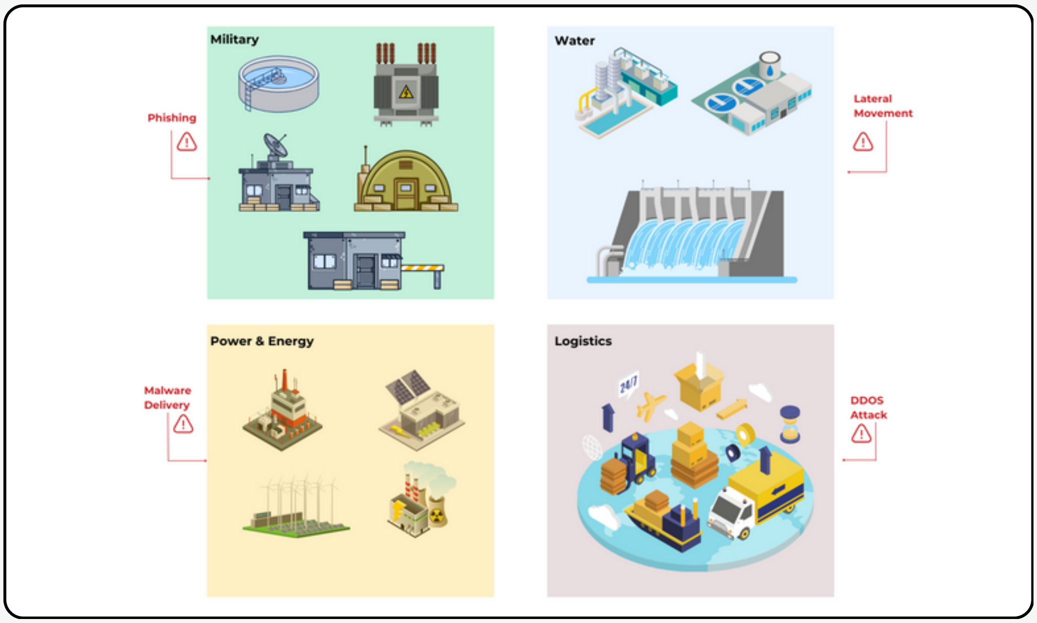
The government sector runs Operational Technology (OT) networks like the commercial sector. Military bases and government facilities have power, water, and logistics infrastructure. Governments directly run water utilities, communications networks, national power grids, pipelines, and other OT infrastructures. Each agency responsible for that infrastructure must secure it per the relevant regulations and guidelines. These facilities are increasingly under attack by bad actors of all types.

The UK's National Cyber Security Center released a report detailing the near-term impact of AI on cyber threats. For governments, the concerning conclusions were that attacks would be more impactful because threat actors could analyze exfiltrated data faster and more effectively and use it to train AI models to more successfully target government networks of all types.

BlastShield Advantages:

- Reconnaissance-Proof Software Defined Perimeter to prevent device discovery and vulnerability exposure with Network Cloaking
- Phishing-Resistant Biometric Multifactor Authentication for Regulatory-Compliant Secure Remote Access
- Delivers Least Privilege Access Policies and prevents Lateral Movement with Network Microsegmentation

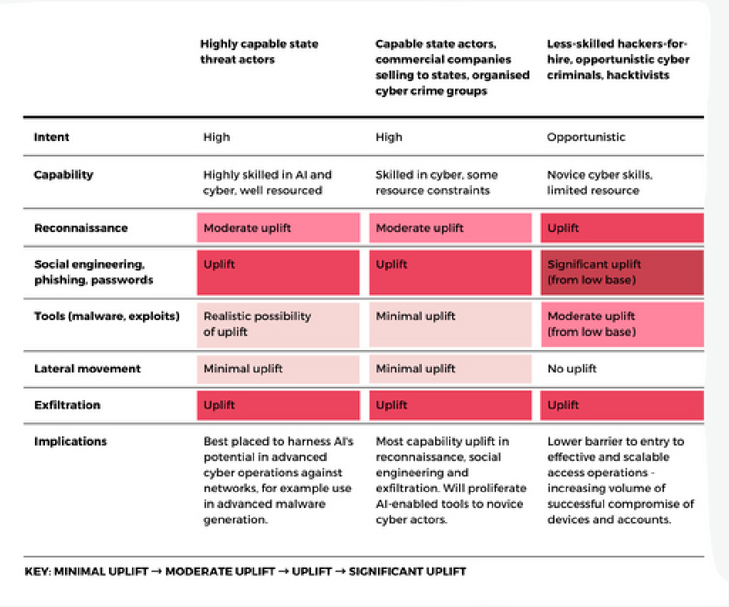
Figure 1: Cyberthreats in Government OT



BlastShield™: AI-Resistant OT Security For Government OT

BlastWave is delivering a radically simplified OT Cybersecurity solution for government OT networks. BlastShield presents a minimal attack surface toward the world, with only biometric-authenticated connections allowed to enter secure OT enclaves

The scale and scope of the risk to government networks, especially its critical OT infrastructure, cannot be underestimated. Multiple reports have detailed the use of AI to aid attacks and hacking of government networks worldwide. The first line of defense in depth for government OT networks must be a solution that resists the initial threat vectors, phishing, reconnaissance, and no-code tools that are uplifted by AI, as reported by the UK government:



	Highly capable state threat actors	Capable state actors, commercial companies selling to states, organised cyber crime groups	Less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists
Intent	High	High	Opportunistic
Capability	Highly skilled in AI and cyber, well resourced	Skilled in cyber, some resource constraints	Novice cyber skills, limited resource
Reconnaissance	Moderate uplift	Moderate uplift	Uplift
Social engineering, phishing, passwords	Uplift	Uplift	Significant uplift (from low base)
Tools (malware, exploits)	Realistic possibility of uplift	Minimal uplift	Moderate uplift (from low base)
Lateral movement	Minimal uplift	Minimal uplift	No uplift
Exfiltration	Uplift	Uplift	Uplift
Implications	Best placed to harness AI's potential in advanced cyber operations against networks, for example use in advanced malware generation.	Most capability uplift in reconnaissance, social engineering and exfiltration. Will proliferate AI-enabled tools to novice cyber actors.	Lower barrier to entry to effective and scalable access operations - increasing volume of successful compromise of devices and accounts.

KEY: MINIMAL UPLIFT → MODERATE UPLIFT → UPLIFT → SIGNIFICANT UPLIFT

With BlastShield, government organizations gain secure remote access, network segmentation, and network cloaking, rendering critical systems undiscoverable to attackers and mitigating the risk of unauthorized access. BlastWave is aligned with NIST 800-53, 800-207 (Zero Trust), CISA Zero Trust Maturity Model, and the DoD Zero Trust Reference Architecture.

Network Cloaking

Network Cloaking ensures that government OT networks of any type are invisible to external threats. Rather than just obfuscating these systems, they do not appear in any scans or probes from a hacker, blocking the initial points of entry for AI-enabled hacking. Network cloaking assists in compliance with specifications like the DoD Zero Trust Reference Architecture. With Network Cloaking, AI-enhanced reconnaissance tools cannot probe into the internal workings of government networks because they have no path to reach the internal OT networks.

Secure Remote Access

BlastShield provides OT Secure Remote Access to government OT systems, enabling real-time management of all systems without exposing them to cyber threats. BlastShield's phishing-resistant MFA biometric authentication protects against GenAI-powered phishing attacks and MFA hijacking. BlastShield creates a full mesh of P2P encrypted tunnels to secure sensitive but unclassified traffic from remote users to government OT networks and any agent-enabled systems, protecting against Man-in-the-middle attacks.

Network Segmentation

BlastShield simplifies the challenge of microsegmentation by creating simple peer-to-peer encrypted and authenticated tunnels to each device or group of devices without complex firewall rulesets. IT and OT network staff and temporary contractors are permitted access to only the systems they are responsible for, and privileges can be granted and revoked in real-time. BlastShield prevents lateral movement by Secure Remote Access users within the network and can even provide lateral movement protection at Layer 2 for local network connections.

About BlastWave

BlastWave prevents AI-powered cyber attacks on critical infrastructure with a unique combination of Zero Trust Cybersecurity capabilities and delivers industrial-grade security with consumer-grade ease-of-use. Visit www.blastwave.com to learn more