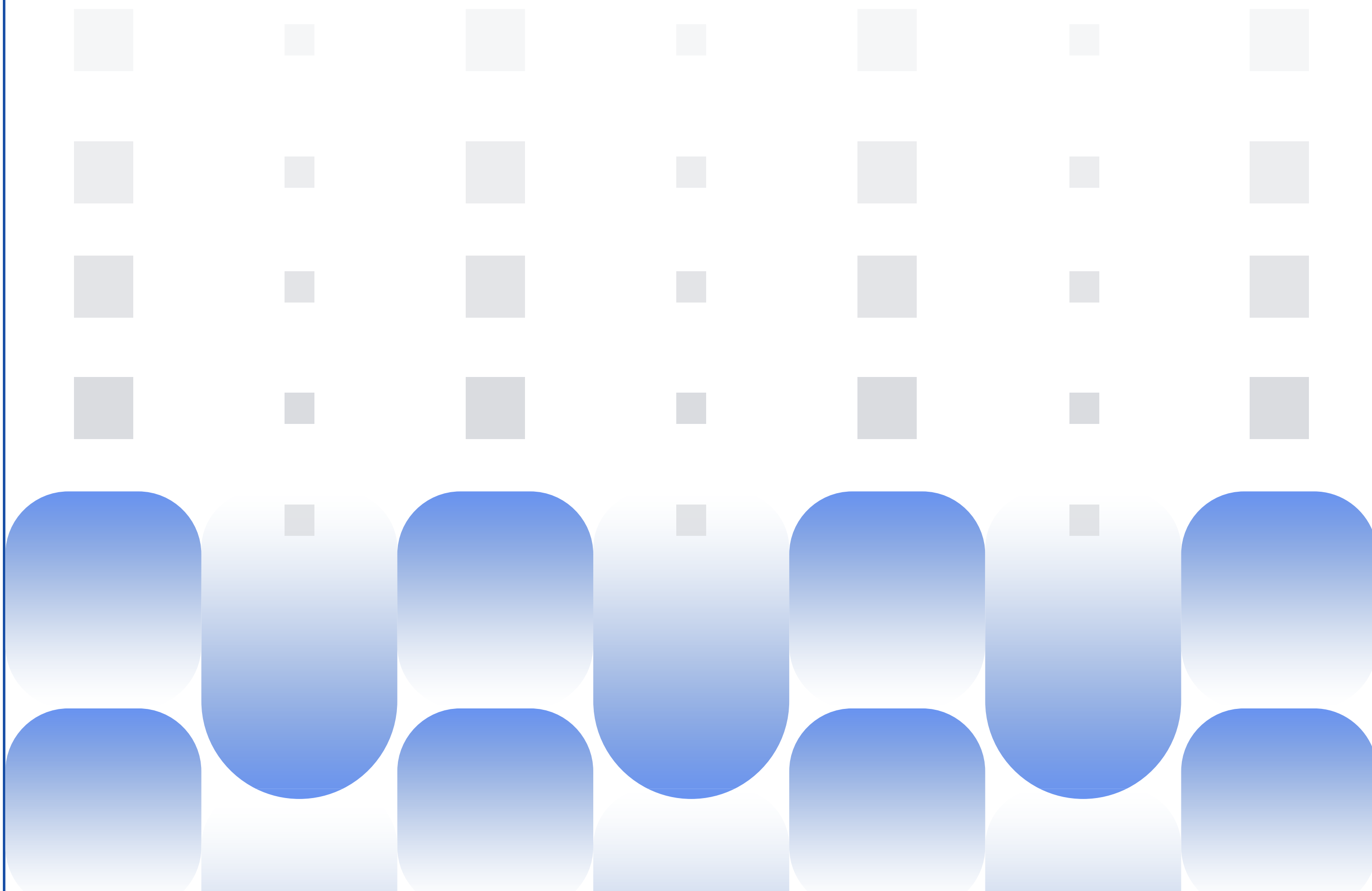
February 2026

Staying Ahead of the Shadows

Digital Resilience in the Era of AI



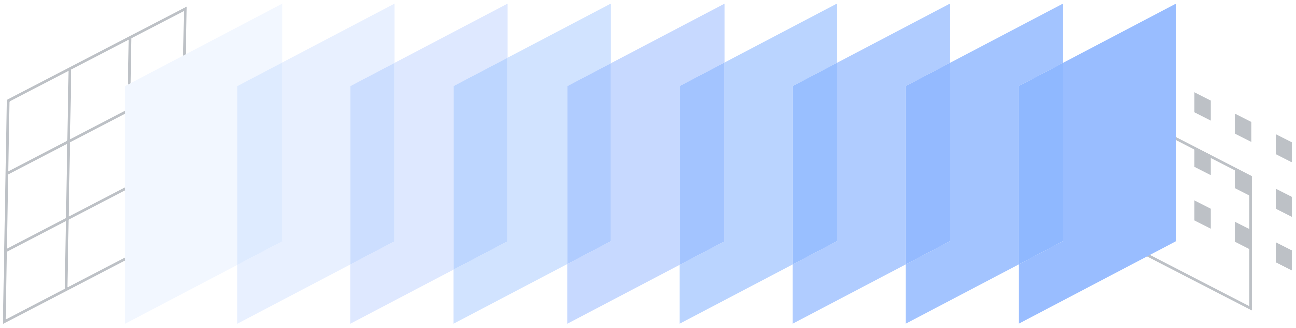
Executive Summary

National security is increasingly digital security. In a complex geopolitical landscape, global competition for AI leadership is more prominent than ever. Democracies must lead the development of this era-defining technology—a necessity made clear by the ongoing war in Ukraine, where digital resilience has proven vital to national defence. To support this, Google is collaborating with defence organisations, equipping democratic partners with the advanced tools necessary to bolster collective resilience.

Current cyber realities underscore the need for a unified defence. Google Threat Intelligence has identified significant cyber threats to U.S. and European defence suppliers and the broader industrial base, with **China and other countries actively targeting defence and aerospace companies**. Producers of next-generation technologies, especially unmanned aerial systems (UASs), have attracted unprecedented attention from threat actors from Russia, China, Iran, and North Korea.

Ransomware, extortion, and other disruptive operations are increasingly targeting the broader manufacturing sector that undergirds the defence industrial supply chain.

Addressing these multi-front threats requires more than just isolated tools, policies, and approaches to global defence: it takes a **unified approach to resilience through innovation**, from the seafloor to the cloud to the user at the edge. It takes a shared digital foundation that transcends borders.



This means taking **a full-stack approach**:

- **Infrastructure: A Resilient Foundation for Digital Innovation** – True resilience begins with a global, redundant network and secure infrastructure. By integrating data centres, planet-spanning subsea and terrestrial cables, and secure-by-design compute and storage infrastructure, Google provides the secure foundation for digital innovation. This infrastructure ensures mission-critical data remains resilient against physical and cyber disruptions, enabling seamless operation without manual intervention.

- **Architecture: A Digital Backbone for Secure and Interoperable Defence** – Modern deterrence depends on the assurance of highly resilient systems. A common cloud architecture built on open standards, open APIs, and interoperable solutions can serve as the "IT backbone" of collective security, transforming the way allies share data, models, and AI-rich applications to accelerate data-driven decisions.

- **Models: The Engines of Competitiveness and Innovation** – AI is the new frontier of strategic advantage, and the pace of transformation is unprecedented. Access to state-of-the-art secure AI platforms is imperative to defence and national security to outpace and outmanoeuvre sophisticated adversaries.

- **Applications: Seamless and Secure Collaboration** – Communication is the nervous system of any operation. Secure, cloud-native solutions like Google Workspace allow government officials and military personnel to collaborate securely from any location, even when traditional on-premises networks are under attack.

- **Security: Future-Proofing the World's Critical Infrastructure** – Secure-by-design infrastructure, architecture, models, and applications are indispensable. Fixing bugs isn't enough; we need to address entire classes of threats. AI can tilt the strategic advantage to defenders, securing vital systems and infrastructure.

It also means taking an agile approach, one based on speed, integration, and control:

Speed is security

The AI revolution, along with consistent advances in semiconductor technology and ubiquitous cloud computing, has made it easier than ever before to rapidly prototype and field test mission-critical software. Democracies can't afford to be locked in multi-year acquisition cycles that slow the fielding of new capabilities; they must adapt to meet the demands of the moment.

Integration through interoperability

The ability to securely share and access data and applications across domains and between allies enhances collective digital resilience. Interoperable systems provide more operational flexibility, increasing resilience under duress.

Control without compromise

Nations can achieve greater resilience and control over their infrastructure and data through public-private partnerships and adoption of state-of-the-art technical solutions, rather than discriminatory requirements that exclude leading innovators.

With so much of the world's critical digital infrastructure in private hands, **resilience is a shared responsibility** and partnerships with industry are critical to accelerating innovation.

Google is committed to its partnerships with democratic governments to build digital resilience and strengthen national security.

Bold and Responsible

Today, Google partners with many of the world's most innovative public and private sector organisations to use innovations, like AI, to tackle hard problems, such as expanding global access to high-quality digital public infrastructure, combating cybercrime and hybrid threats targeting critical infrastructure, protecting journalists and dissidents from online surveillance and censorship, and building information systems that deliver both global scale and local control.

In 2018, we were the first company to publish a set of Responsible AI Principles, which guide our work in building technologies that advance the collective security and resilience of our democratic partners and a safer world for all.

Google's AI Principles[1]

1. Bold innovation.

We develop AI that assists, empowers, and inspires people in almost every field of human endeavour. AI drives economic progress, improves lives, enables scientific breakthroughs, and helps address humanity's biggest challenges.

2. Responsible development and deployment.

Because we understand that AI, as a still-emerging, transformative technology, poses evolving complexities and risks, we pursue AI responsibly throughout the AI development and deployment life cycle – from design to testing to deployment to iteration, learning as AI advances and uses evolve.

3. Collaborative progress, together.

We make tools that empower others to harness AI for individual and collective benefit.

The Threat to the Defence Industrial Base

Google Threat Intelligence Group (GTIG) observes **several distinct areas of focus** in adversarial targeting of the defence industrial base in democratic nations.

The following findings typify just some of the tactics, techniques, and procedures we observe:

- Consistent targeting of defence entities involved in testing and deploying next-generation technologies on the battlefield in the Russia-Ukraine War, and in particular, UASs and counter-UAS technologies. GTIG has observed direct attempts to **compromise defence companies**, potentially as an entry point into the military units they partner with, as well as attempts to compromise military targets through the spoofing of defence tech products and systems. In one campaign associated with Russia-nexus actor UNC5976, the actor registered hundreds of domains spoofing Western defence contractors, possibly to support credential harvesting operations. The primarily European defence contractors are involved in a range of defence technologies such as aviation, unmanned aircraft systems, precision munitions, and intelligence, surveillance, and reconnaissance (ISR) systems.

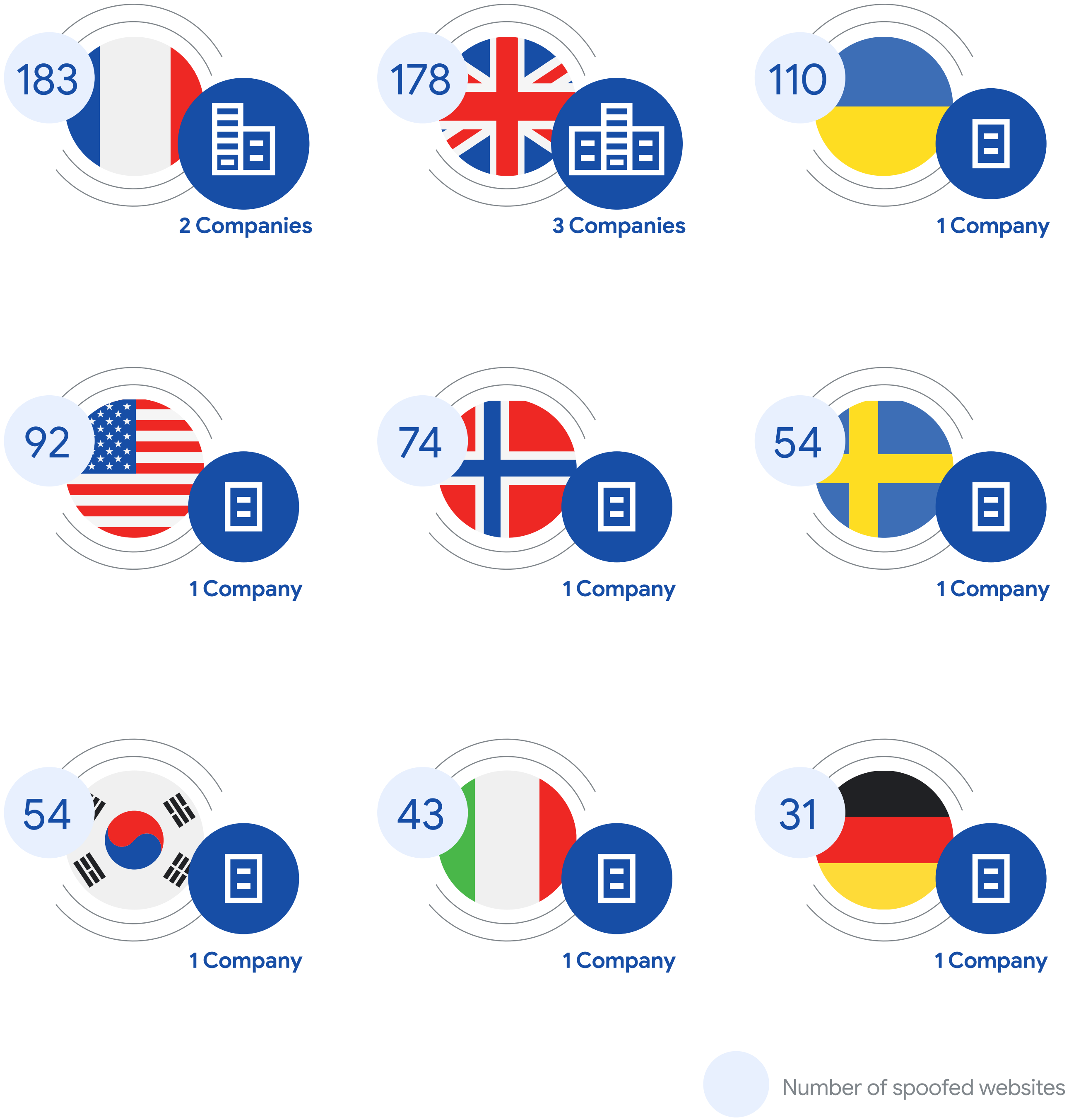
- The **direct targeting of employees and exploitation of the hiring process** has emerged as a theme across global defence and aerospace firms. From the North Korean IT worker threat,[2] to the spoofing of recruitment portals, employee targeting remains a common threat vector employed by a number of cyber espionage actors.

- Among **cyber espionage** intrusions over the threat activity from **China-nexus groups continue to represent by volume the most active threat** to entities in the defence industrial base. While these intrusions continue to leverage an array of tactics, campaigns from actors such as UNC5221 highlight how the **targeting of edge devices** as a means of initial access has increased as a tactic by this category of adversary, and poses a risk to the defence and aerospace sector.

- Since 2020, **manufacturing has been the data leak sites** – where threat actors publish stolen victim data – associated with ransomware and extortive activity. Beyond defence and aerospace organisations, manufacturing companies that produce **dual-use components** for defence applications remain a target. Cyber risks to NATO's industrial supply chain can undermine NATO's collective defence capacity if they threaten the ability to surge components where they're needed during crises.

UNC5976 Spoofed Defence Domains by Country

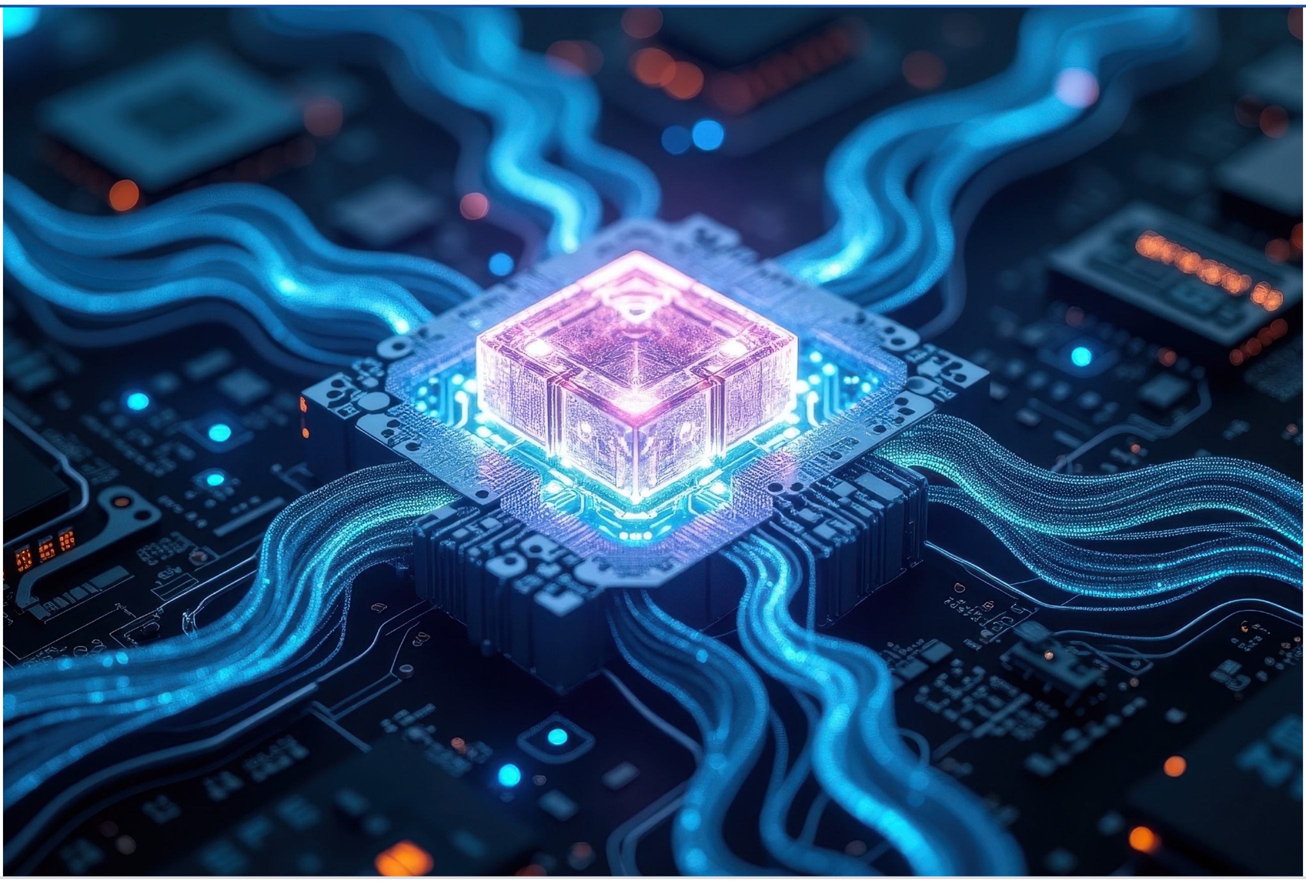
Credential Harvesting Infrastructure Spoofing Aerospace and Defence Firms



Information operations remain an area of attention for Google security teams as a potential force multiplier for hybrid operations.

Following public reporting on drone incursions into Polish airspace in October 2025, GTIG linked the drone activity to a coordinated, Russia-aligned influence operation promoting counter-narratives that blamed Poland and NATO for the poor state of relations with Russia.[3]

As Europe reforms its defence sector, GTIG's unique visibility into cyber and information operations and our unbiased analysis can aid policymakers in formulating a calibrated policy response.



> "Modern conflict no longer rewards the side with the most data. It rewards a side with the ability to connect it, understand it, and act on it first. Cloud adoption is not a technical upgrade discussed by specialists in quiet rooms; it is an operational and strategic imperative, and one that will shape deterrence crisis management and ultimately the credibility of our collective defence."[4]

Jean-Charles Ellerman-Kingcombe
NATO Assistant Secretary General

Infrastructure
A Resilient Foundation for Digital Innovation

Escalating cyber and hybrid threats demand solid foundations and global scale to defend the efficient flow of information. Google's investments in data centres, subsea and terrestrial cables, high-efficiency semiconductors called Tensor Processing Units (TPUs), and custom network and workload management software have proven central to our mission of organising the world's information.[5]

Google's globe-spanning network affords our customers and users strategic resilience in times of crisis or uncertainty. Its scalable software control plane instantly reroutes traffic around faults without manual intervention. Customers can route their traffic through our more than 200 points of presence globally and keep that traffic on our proprietary, low-latency network, only exposing it to the public Internet at the last possible moment.[6]

Spotlight
Subsea Cables

About 99% of the world's intercontinental Internet traffic and more than $12 trillion in financial transactions flow through approximately 600 subsea cables each day. These lines are the invisible arteries of the global digital economy.[7] Nevertheless, an estimated 150-200 cable failures occur annually. While most are caused by inadvertent human activity like fishing, deliberate threats are on the rise.

The key to subsea resilience is a robust and redundant network that is not vulnerable to a single cable failure, regardless of the cause.

At Google, we approach resilience as a holistic network architecture strategy, rather than just "hardening" individual cables, focusing on:

- **State-of-the-art technology:** Our transatlantic Grace Hopper cable, completed in 2021, is one of the highest -capacity cables in the world, delivering more than 350 terabits per second between New York, Spain, and the UK.[8]

- **Global network:** 34 subsea projects are core to our network of alternative digital pathways, including expanded interconnections in Hamina, Finland, to maximise resilience in the Baltic.

- **Intelligent redundancy:** We build concurrent paths for instant traffic redistribution. When a 2025 climatic event severed multiple regional lines off West Africa, Google's Equiano cable stayed online because its route was strategically isolated from those hazards.

- **Partnerships:** We collaborate with governments and seabed users – from wind farm operators to military and fishing groups – to ensure the safe, coordinated co-existence of all critical maritime infrastructure.

Google's hyperscale cloud leverages redundancy and massive failover capacity to maximise operational resilience in the event of disruptions to any part of the network, whether that be the result of a technical outage or a hybrid threat. The cloud's inherent economies of scale expand access to state-of-the-art technologies like AI-powered threat detection and post-quantum cryptography (PQC) while driving down the cost to customers.[9]

Google Cloud's portfolio of Sovereign Cloud solutions was built for defence organisations, the public sector, critical infrastructure operators, and global enterprises with high-performance missions and strict compliance requirements. They allow our customers to innovate using state-of-the-art AI capabilities without compromising control:[10]

- **Google Cloud Data Boundary** puts customers in control of their data through data residency and customer-managed security controls. Customer control of encryption keys, combined with access transparency logging, is a strong and effective technical measure against extraterritorial data access.
- **Google Cloud Dedicated** delivers a cloud platform designed to meet local sovereignty requirements, managed by trusted local and regional partners. Google Cloud partnered with French defence technology leader, Thales, to launch a first-of-its-kind Trusted Cloud by S3NS. S3NS is a European cloud provider subject exclusively to EU law, and in December 2025 became the first partnership to achieve the rigorous SecNumCloud certification.[11]
- **Google Distributed Cloud Air-Gapped** is a fully-isolated platform operated by a trusted sovereign partner and tailored for customers in the defence and national security sectors.

Google backs these technical solutions with contractual and procedural safeguards. We are committed to using all legal avenues available to limit, modify, or object to extraterritorial requests for customer data, and to notifying customers of such requests where permissible.

Spotlight
Edge Computing - Google Distributed Cloud Air-Gapped

Mission owners operating at the tactical edge where connectivity is limited or contested can't afford to rely on centralised data processing. It's critical to push the processing power for AI and data analytics to the edge, where speed, performance, and low latency can accelerate time-to-decision and confer a strategic advantage.

Google's air-gapped cloud (GDC-AG) is becoming a partner of choice for the defence community:

- **NATO Communication and Information Agency (NCIA)** selected GDC-AG in a first-of-its-kind contract to power its new Joint Analysis, Training, and Education Centre (JATEC).[12]
- **The U.S. Department of War** has accredited GDC-AG to provide critical computing and AI capabilities at the tactical edge, including at one of its highest levels of security: Impact Level 6 (IL-6).[13]
- **The German Armed Forces** announced the acquisition of GDC-AG devices to power mission-critical business applications in its private cloud.[14]
- **The United Kingdom's Ministry of Defence** chose GDC-AG to provide its workforce access to advanced AI and analytics while enforcing strict data residency and security.[15]
- **Australia's Ministry of Defence** entered into a partnership with Google Cloud to deliver air-gapped cloud capabilities to "enable faster, smarter, and more secure Defence operations."[16]

Google's air-gapped cloud (GDC-AG) was designed with defence and national security organisations in mind. It is a "cloud-in-a-box" solution that can run disconnected from the public Internet. It allows for:

Complete independence: Defence organisations can run workloads without reliance on connectivity to the public Internet or to Google, offering unprecedented control and resilience in case of service disruptions or in a contested-bandwidth environment.

Advanced tools anywhere: For the first time, Google's world-class AI models, Enterprise Search, and pre-trained APIs (e.g. Translate, Speech-to-Text) are available to customers operating in classified or highly sensitive environments.

Plug-and-play: Unlike proprietary systems that lock users in, GDC-AG is built to be interoperable, maximising data and application portability.

Train once, deploy everywhere: GDC-AG uses an open, containerised architecture, so an AI model developed by one nation can be easily shared and deployed by allies, across cloud and edge infrastructure, without costly re-engineering.

Architecture
A Digital Backbone for Secure and Interoperable Defence

The security of NATO and European nations depends on the speed and efficacy of their **collective response** and a shared digital foundation that transcends borders. NATO's 2030 Strategy emphasises the commercial cloud's ability to extend a common data architecture – a "Digital Backbone" – from headquarters to multiple clouds to the tactical edge.[17]

Defence organisations must move beyond rigid, siloed infrastructure toward a flexible, survivable fabric. At Google Cloud, we call this concept "Hybrid Sovereign Mesh." This unified ecosystem integrates diverse computing environments – from hyperscale data centres, multi-cloud platforms, dedicated cloud installations, air-gapped platforms, and tactical edge environments – into a single, secure, interoperable continuum.

Spotlight

Google's Sovereign Hybrid Mesh Architecture

Google's unique Sovereign Hybrid Mesh capabilities fuse the cloud and edge, giving defence partners the flexibility to innovate while meeting strict compliance requirements. It allows developers to build and deploy AI-rich applications across multiple Google Sovereign Cloud solutions, while enabling the secure sharing of data and models across network boundaries and data classification tiers.

The Mesh directly answers the NATO Digital Backbone vision by enabling secure data manoeuvrability across compliance boundaries and coalition partners. Rather than trapping data in disconnected classification tiers, the Mesh utilises interoperability gateways to bridge domains securely, ensuring that mission-critical functions flow to where they are needed most.

Key Operational Mechanisms:

Secure Interoperability: The Mesh enforces strict policy controls on data that crosses classification tiers. This allows lower-classification inputs, such as open-source intelligence, to feed higher-classification analysis. Inversely, high-side insights can be sanitised and shared with coalition partners via cross-domain solutions.

Robust Cryptography: Data traversing the Mesh is protected by hybrid encryption, combining both National Security Agency-accredited protocols and NIST-approved PQC algorithms, ensuring that intercepting infrastructure traffic yields no intelligence value to adversaries.

Granular Control: Cross-domain filtering and data loss prevention tools log and inspect content in real-time, stripping sensitive metadata or blocking unauthorised transfers before they cross security boundaries.

This architecture transforms static infrastructure into a dynamic strategic asset, allowing commanders to leverage global AI innovation while maintaining absolute control over their most critical secrets.

Cultivating interoperability throughout the tech stack and between allies enables a “win together” mindset.

A common cloud architecture built on interoperable solutions like GDC-AG can serve as the “IT backbone” of collective security, transforming the way allies share data, models, and AI-rich applications to accelerate data-driven decisions. This is enabled through adoption of open standards, open APIs, shared encryption protocols, and common data classification levels across national compliance frameworks. The ability to run workloads across multiple cloud and edge platforms and providers allows defence organisations to reduce fragmentation, avoid vendor lock-in, mitigate concentration risks, and manage costs.

Spotlight

Defense Logistics Agency

The U.S. Defense Logistics Agency (DLA) manages the end-to-end global flow of equipment for all five U.S. military services – a massive undertaking where speed and accuracy can save lives. Using Google Cloud as their foundational platform, the DLA is breaking down data silos and structuring their data within a unified data fabric. With AI tools such as Vertex AI and BigQuery, DLA is replacing slow, manual paperwork with automated and AI-assisted workflows that provide real-time supply chain intelligence. Partnering with Google Cloud enables the DLA to transform its vast sea of data, transforming the agency from a logistics operations agency into a data-driven logistics information agency.

This enables DLA's workforce to focus on key functions, including:

Forecasting demand for key parts and materiel amid changes in the global political landscape, which helps to mitigate shortages and manage costs;

Evaluating the performance of suppliers, enabling planners to identify risks from unreliable vendors;

Reconciling inventories against financial records to identify potential data quality issues in order to reduce risk and avoid audits; and

Enhancing cybersecurity readiness by continually monitoring assets for exposure, enabling more proactive threat hunting and a more in-depth understanding of the Agency's exposure to cyber risks.

Models
The Engines of Competitiveness and Innovation

AI represents perhaps the most monumental technological advancement in a generation, with profound implications for the global economy and international security. The pace of the transformation is unprecedented: some research suggests that AI models' capabilities double with every generation – roughly every seven months.[18] This makes access to state-of-the-art technologies imperative to every nation's defence and national security.

Google and our world-leading frontier research lab, Google DeepMind, are developing the most capable and general-purpose AI models available. Gemini 3.0, released in November 2025, outperforms alternatives in leading benchmarks for inference and multimodal reasoning.[19]

As we pursue a bold and responsible vision, we collaborate with government partners, such as the UK AI Safety Centre and the U.S. Center for AI Standards and Innovation (CAISI), to help establish standards for AI governance and empower nations to adopt AI safely.

Through our Frontier Safety Framework, we're constantly evaluating our models for safety risks and implementing mechanisms to detect and mitigate them.[20] Google is also committed to partnering with governments to unlock the power of AI on their own terms. In December 2025, for example, Google DeepMind signed a memorandum of understanding with the UK Government to accelerate access to frontier AI and translate AI advances into public benefit.[21]

Spotlight

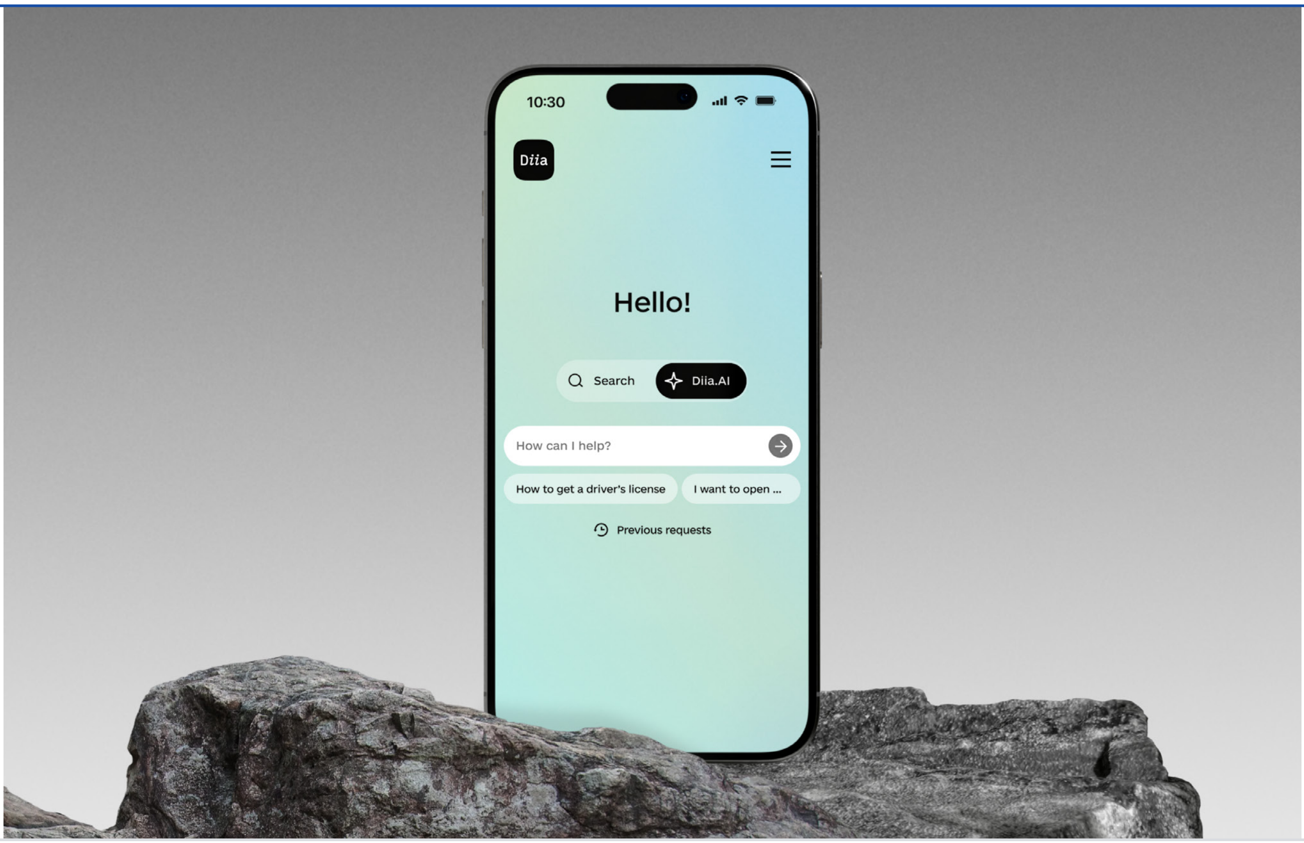
GenAI.mil

Google is partnering with the U.S. Department of War (DoW) to bring modern AI to more than three million military and civilian personnel. Through the Pentagon's GenAI.mil programme, DoW staff can now use Gemini for Government to handle daily tasks and boost productivity just as they would in the private sector.[22]

Gemini can help distill massive amounts of internal data, summarise emails and documents, and even use "agentic" tools – AI assistants that enable users to automate complex office work. Gemini for Government is certified at FedRAMP High and DoW Impact Level 5, ensuring that DoW data stays private and secure within a dedicated Google Cloud enclave.

> Google Cloud customers have the flexibility to run powerful AI models, such as Gemini, across our Sovereign Cloud solutions, with full data residency controls and oversight by trusted local partners, such as S3NS.

Our open-weight models, such as Gemma, offer our partners the ability to run Google's world-class AI on their own sovereign infrastructure or on Google's, including our fully-isolated GDC-AG platform. We're also partnering with governments and research institutes around the world to develop localised models fine-tuned on national data sets to better reflect local languages and practices.[23]



Spotlight

Diia.AI

Since the start of the war, the Ministry of Digital Transformation has transformed Diia into a true "everything app," built to meet today's new challenges — with digital passports, 30+ other services in the app and 165+ on the Diia portal, including one of the fastest business registration processes, online marriage, financial aid, and other essential services.[24]

The Ministry now integrates Gemini into the Diia platform – Diia.AI, the world's first AI assistant performing real government services, where Ukrainians use a single chat-based interface to access information and get documentation without having to transmit sensitive personal information outside the Ministry's secure platform.[25]

"Google is our strategic partner in this effort. Together, we collaborate across education, digital skills, AI, and startup support," wrote Mykhailo Fedorov, Ukraine's First Deputy Prime Minister — Minister of Digital Transformation (now the Minister of Defence of Ukraine) in an October 2025 blog post. "Launching Diia.AI on Gemini has become a global case study for how public-private partnerships can deliver real AI solutions, not just for the government, but for millions of people."[26]

In December 2025, the Ministry and telecom leader Kyivstar announced the next AI milestone: the "National LLM" will be built on Google's open-weight Gemma 3 model.[27] While Gemini powers the public interface, the National LLM utilises Gemma 3 to handle sensitive internal processing and sovereign data tasks.

Applications
Seamless and Secure Collaboration

Applications are portals to the digital world: they're where infrastructure, data, and models converge to meet the needs of the end user.

Google's own applications, such as Google Workspace, were built in the cloud: they inherit strong embedded security controls, the reliability and redundancy of our global network, and the benefits of a highly-iterative software lifecycle. Unlike with legacy software, new features and security fixes are continuously pushed to end users without action required on their part – making state-of-the-art security appear invisible.[28]

Spotlight

Ukrainian Government Chooses Google Workspace

In early 2022, Ukrainian data facilities and communication channels became prime targets for Russia's cyber, ground and missile offensive, directly threatening the Ukrainian Government's ability to collaborate – including sending emails and sharing documents – securely over official channels. By early spring Ukrainian civil servants began switching over to their consumer Google Workspace accounts to conduct official business. Unlike localised infrastructure, Workspace remained reliable and accessible from any location with an Internet connection. Crucially, it also offered superior protection against Russian malware attacks that were targeting on-premises systems.

In response, Google partnered with the Digital Ministry to provide 50,000 Workspace Enterprise licences.[29] This fortified the government's digital defence through access to Zero Trust security, which continuously scans all users, identities, and devices before granting access to data and network resources.

Ultimately, this transition ensured that while the government's physical infrastructure faced constant threat, its digital state remained fully operational.

Security
Future-Proofing the World's Critical Infrastructure

Security is at the core of our Infrastructure, Architecture, Models, Applications – everything we do at Google.[30] We don't just fix bugs – we eliminate entire classes of threats.

Cyberattacks are increasingly a tool of geopolitical coercion, often targeting critical infrastructure like hospitals, schools, telecommunications, and the energy grid to sow chaos and confusion.[31] Threat actors have seized on AI's ability to craft more credible social engineering lures, to generate new malicious scripts, and even to automate aspects of the cyber kill chain, enabling them to target organisations with greater scale, precision, deniability and sophistication than ever before.[32]

Google launched the AI Cyber Defense Initiative in 2024 and pledged to partner with governments and experts around the world to help defenders use AI to take the upper hand in the fight for a more secure cyberspace.[33]

We continue to deliver on our commitments to strengthening global security through:

- Developing industry standards and best practices for building secure-by-design AI systems, including the Secure AI Framework (SAIF).[34]
- Producing cutting-edge research into advanced applications for AI in security and releasing open source tools to uplift security at the ecosystem level.[35]
- Embedding strong AI-based protections into Google commercial products and services.[36]
- Investing in university partnerships to provide free AI and cybersecurity training for students and job seekers.[37]
- Publishing threat intelligence into adversarial use of AI,[38] including our own AI models, and engaging with government and industry leaders to combat threats.

Spotlight
Secure AI Framework (SAIF)

As AI technology evolves, governments and industry need standards for building and deploying AI securely and responsibly. The Secure AI Framework (SAIF) is a conceptual framework modelled on Google's own internal processes that guides AI developers to identify potential risks and embed secure-by-design practices in their applications.[39] In 2025, we updated SAIF to identify and address the unique security and privacy challenges posed by agentic AI so that organisations can experiment with confidence. In collaboration with our partners in the Coalition for Secure AI (CoSAI), we've also built and shared a comprehensive toolkit for developers that includes open source resources and guidance for designing, building, and evaluating AI models responsibly.[40]

Spotlight
AI Security Agents

Agentic AI has tremendous potential to transform the way organisations defend themselves. Big Sleep, a Google-built AI agent released in 2024, is capable of independently scanning millions of lines of source code to find and catalogue previously undiscovered vulnerabilities, known as 0days.[41] CodeMender, released in 2025, not only finds bugs in open-source code, but also writes patches completely autonomously.[42] AI agents like these allow defenders to massively scale efforts to improve software quality and vulnerability management upstream in the development process.

Public-private partnerships remain critical to identifying shared risks and building joint preparedness for emerging threats. Our GTIG and Mandiant Consulting teams maintain robust partnerships with more than 80 governments, including multiple U.S. Government agencies, the European Agency for Cybersecurity (ENISA), and NATO.

Mandiant, notably, was on the ground in Kyiv months before the invasion, working side-by-side with the Ukrainians to prepare for asymmetric cyber conflict.[43]

Mandiant's around-the-clock support to Ukraine's cyber defenders helped them harden their networks, remove Russian hackers from their critical infrastructure, and, in some cases, deter further aggression. Google continues to play a critical role in Ukraine's cyber defence through incident response efforts, support for training and capacity-building initiatives, and providing security keys to high-risk individuals. Publishing threat analysis on Russian activity in Ukraine supports cyber defence missions around the globe.[44]

Spotlight

Post-Quantum Cryptography

Google is working with governments, critical infrastructure operators, and academic experts around the world to prepare for a post-quantum future. Powerful quantum computers could threaten the cryptography that protects global communications and commerce. To prevent this, we need to collectively succeed in transitioning the world to quantum-safe cryptography first.[45]

This issue demands greater attention and urgency than it has so far received. Powerful nation-states and advanced cybercriminals may already be collecting global encrypted communications in bulk to decrypt them in the future once a cryptographically relevant quantum computer (CRQC) is made available – a concept known as "harvest-now-decrypt later." Further, while the cryptographic transition could take anywhere from five to ten years, it's possible that a viable CRQC – and the veritable "Q Day" – could arrive sooner than expected.[46]

Google began its cryptographic modernisation in 2016, and ever since we've led the industry in implementing PQC across high-impact use cases, such as encryption in-transit, firmware signatures, software signatures, public key infrastructure, and tokens.[47]

We remain committed to collaborating with governments and organisations like NATO to accelerate the global PQC transition, promote harmonisation of global cryptographic standards, and provide guidance and resources to Google customers and the broader software ecosystem.

Policy Recommendations

Governments have a strong role to play in ensuring a unified approach to resilience.

1. Speed is Security: Accelerating Innovation to Outpace the Threat

Technological superiority can't be delivered through traditional procurement cycles.

Governments should:

Modernise Procurement:

Commit to the NATO Rapid Adoption Action Plan's goal of reducing procurement timelines from decades to under 24 months, including through mutual recognition of national standards and certification, joint procurement and rapid field testing.[48]

Catalyse Infrastructure Growth:

Delivering resilience is not just about better infrastructure, it's more infrastructure. For the global subsea cable network to be truly diverse and resilient, we need expedited and streamlined permitting regimes both for cables and repair ships as well as a close public-private partnership to evaluate how to best monitor their integrity without increasing their vulnerability.

Operationalise Lessons Learned:

Formalise programmes, such as those informed by the war in Ukraine, to accelerate real-world technological adaptations into military doctrine and public-private defence partnerships. The planned NATO–Ukraine Joint Analysis, Training and Education Centre (JATEC) will become a central force in NATO's innovation ecosystem, connecting urgent battlefield needs to agile technological response. Foundational partnerships, such as the one between NATO's Communication and Information Agency (NCIA) and Google Cloud, are currently laying the digital groundwork to deliver on this mission.[49]

2. Integration through Interoperability: Building a Shared Backbone for Collaboration

The ability to securely share and access data across domains, partners, and allies is indispensable for collective digital resilience. Interoperable systems provide more operational flexibility, increasing resilience. Integration prevents the creation of new data silos and mitigates the risk of vendor lock-in.

Uplift the Entire Ecosystem:

Governments should invest in modern, cloud-based infrastructure to replace vulnerable legacy systems. This creates a positive growth cycle of security, including AI-powered threat detection and post-quantum cryptography, which protects the government and the small and medium-sized businesses, supporting the national economy.

Combat Fragmentation and Lock-In:

National procurement policies should set standards for interoperability and data portability by design – through open standards, open APIs, shared encryption protocols, and common data classification levels across national compliance frameworks – as an alternative to re-engineering fragmented systems once in production. The ability to run workloads across multiple cloud platforms and providers allows defence organisations to avoid vendor lock-in, mitigate concentration risks, and manage costs.

Engage Strategic Partnerships:

Identify clear channels for industry collaboration before a crisis occurs. These partnerships should focus on mapping digital assets, joint testing, and sharing intelligence on emerging cyber-physical threats.

3. Control without Compromise: Resilience through Public -Private Partnerships

Nations can achieve greater resilience and control over their infrastructure and data through public-private partnerships and adoption of state-of-the-art technical solutions, rather than discriminatory requirements that exclude leading innovators.

Ensure a Level Playing Field:

Avoid discriminatory "buy local" requirements that may unintentionally create shortages in compute, expertise, and access to state -of-the-art innovation. Instead, set a high bar for security through international standards and modern controls like customer-managed encryption.

Deploy Sovereign-Ready Solutions:

Leverage proven templates for air-gapped, AI-ready infrastructure to meet strict data residency requirements without sacrificing the power of frontier AI.

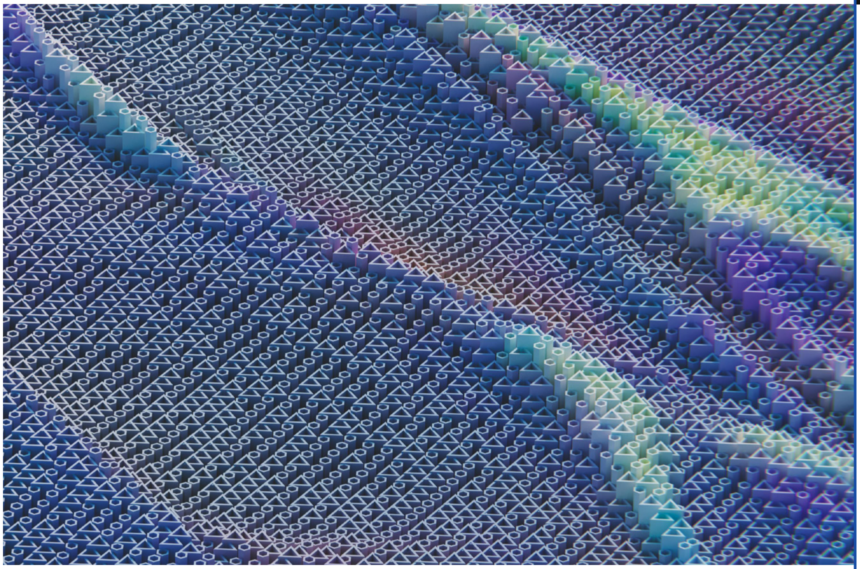
Foster Technical Expertise:

Invest in university, research, and industry partnerships to build a workforce capable of implementing, managing, and innovating with sovereign technologies, ensuring that the "warrior ethos" is backed by the necessary digital fluency.

Conclusion

The digital frontier is no longer on the horizon; it's the current terrain upon which global security and national sovereignty will be decided.

Leading on that frontier will take a unified approach to innovation, from the seafloor to the cloud to the user at the edge. It will take rapid access to state-of-the-art technology and security at all levels of the stack. And it will take speed, choice, interoperability, control, and partnerships. Google remains dedicated to a bold and responsible vision: building the secure, interoperable foundation that allows democracies to innovate with confidence, defend with precision, and lead with excellence. Google and our defence sector partners stand ready to co-design resilient, compliant, interoperable cloud platforms and solutions to fit democracies' strategic and tactical defence goals.



[1] AI Principles - Google AI: https://ai.google/principles/

[2] DPRK IT Workers Expanding in Scope and Scale | Google Cloud Blog: https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale

[3] Pro-Russia Information Operations Leverage Russian Drone Incursions into Polish Airspace | Google Cloud Blog https://cloud.google.com/blog/topics/threat-intelligence/pro-russia-information-operations-drone-incursions

[4] Recording: NATO and the Cloud | Royal United Services Institute: https://www.rusi.org/research-event-recordings/recording-nato-and-cloud

[5] A peek behind Colossus, Google's file system | Google Cloud Blog: https://cloud.google.com/blog/products/storage-data-transfer/a-peek-behind-colossus-googles-file-system

[6] Under the sea: Building Google's fiber optic network | Google Cloud Blog: https://cloud.google.com/blog/topics/developers-practitioners/googles-subsea-fiber-optics-explained

[7] Securing Global Communications: An Examination of Foreign Adversary Threats to Subsea Cable Infrastructure | Telegeography blog: https://blog.telegeography.com/hubfs/Tim%20Stronge%20Written%20Congressional%20Testimony%20%7C%20TeleGeography.pdf

[8] Our Grace Hopper subsea cable has landed in the UK | Keyword Blog: https://blog.google/around-the-globe/google-europe/united-kingdom/our-grace-hopper-subsea-cable-has-landed-uk/

[9] 9 megatrends drive cloud adoption—and improve security for all | Google Cloud Blog: https://cloud.google.com/blog/products/identity-security/8-megatrends-drive-cloud-adoption-and-improve-security-for-all

[10] Google advances sovereignty, choice, and security in the cloud | Google Cloud Blog: https://cloud.google.com/blog/products/identity-security/google-advances-sovereignty-choice-and-security-in-the-cloud

[11] S3NS announces SecNumCloud qualification for PREMI3NS, its trusted cloud offering | Thales Group: https://www.thalesgroup.com/en/news-centre/press-releases/s3ns-announces-secnumcloud-qualification-premi3ns-its-trusted-cloud

[12] NATO and Google Cloud Sign Multi-Million Dollar Deal for AI-Enabled Sovereign Cloud - Nov 24, 2025: https://www.googlecloudpresscorner.com/2025-11-24-NATO-and-Google-Cloud-Sign-Multi-Million-Dollar-Deal-for-AI-Enabled-Sovereign-Cloud

[13] Department of the Navy Awards Cloud Computing Task Orders for Google Cloud Platform, Oracle Cloud Infrastructure: https://www.navy.mil/Press-Office/News-Stories/display-news/Article/4345891/department-of-the-navy-awards-cloud-computing-task-orders-for-google-cloud-plat/

[14] Bundeswehr relies on Google Cloud | heise online: https://www.heise.de/en/news/Bundeswehr-relies-on-Google-Cloud-10397526.html

[15] Google Cloud Awarded Landmark Sovereign Cloud Contract with UK Ministry of Defence: https://www.googlecloudpresscorner.com/2025-09-11-Google-Cloud-Awarded-Landmark-Sovereign-Cloud-Contract-with-UK-Ministry-of-Defence

[16] Defence signs Deed of Standing Offer with Google Australia for Defence hyperscale cloud: https://www.defence.gov.au/news-events/releases/2025-12-19/defence-signs-deed-standing-offer-google-australia-defence-hyperscale-cloud

[17] NATO'S Digital Transformation Implementation Strategy | NATO Official text; NATO Digital Backbone: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/17/natos-digital-transformation-implementation-strategy

[18] Artificial Intelligence Index Report 2025 | Stanford HAI: https://hai.stanford.edu/assets/files/hai_ai_index_report_2025.pdf

[19] A new era of intelligence with Gemini 3 | Keyword Blog: https://blog.google/products-and-platforms/products/gemini/gemini-3/#gemini-3-deep-think

[20] Updating the Frontier Safety Framework - Google DeepMind: https://deepmind.google/blog/updating-the-frontier-safety-framework/

[21] Our partnership with the UK government - Google DeepMind: https://deepmind.google/blog/strengthening-our-partnership-with-the-uk-government-to-support-prosperity-and-security-in-the-ai-era/

[22] 'Gemini for Government': Supporting U.S. Government's AI Transformation | Google Cloud Blog: https://cloud.google.com/blog/topics/public-sector/introducing-gemini-for-government-supporting-the-us-governments-transformation-with-ai

[23] AI Singapore makes AI more inclusive for Southeast Asia with Gemma 2 - Google DeepMind: https://deepmind.google/models/gemma/gemmaverse/sea-lion/

[24] Ukraine's Digital Transformation: Innovation for Resilience | Harvard Kennedy School: https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience

[25] When the State Leads on AI: What Diia.AI and ePermit Tell Us About Agentic Public Services | by Pavlo Sydorenko | Medium: https://medium.com/@pavlo_sydorenko/when-the-state-leads-on-ai-what-diia-ai-and-epermit-tell-us-about-agentic-public-services-a27b5a30ecfb

[26] A Vision for AI in Government: How Ukraine is Leading the Way with AI in Public Services: https://publicpolicy.google/article/ukraine-ai-public-service/

[27] Kyivstar and Ukrainian Ministry of Digital Transformation Select Google Gemma as the Foundation for Ukraine's National LLM | VEON: https://www.veon.com/newsroom/press-releases/kyivstar-and-ukrainian-ministry-of-digital-transformation-select-google-gemma-as-the-foundation-for-ukraines-national-llm

[28] Security Summit: Google Cloud charts a safer future | Google Cloud Blog: https://cloud.google.com/blog/products/identity-security/security-summit-google-cloud-charts-a-safer-future

[29] Mykhailo Fedorov announced new support package for Ukraine from Google: https://www.kmu.gov.ua/en/news/2-mln-dolariv-na-tsyfrovu-osvitu-ta-50-tysiach-litsenzii-google-workspace-mykhailo-fedorov-povidomyv-pro-novyi-paket-pidtrymky-ukraini-vid-google

[30] 7 ways we're incorporating security by design into our products and services: https://blog.google/technology/safety-security/google-secure-by-design-pledge/

[31] Poland Cyberattack Nearly Triggered Blackout, Minister Warns; NHS ransomware attack contributed to patient's death: https://www.bbc.com/news/articles/cp3ly4v2kp2o

[32] Cloud CISO Perspectives: Data-driven insights into AI and cybersecurity | Google Cloud Blog: https://cloud.google.com/blog/products/identity-security/cloud-ciso-perspectives-data-driven-insights-ai-cybersecurity

[33] Sundar Pichai: AI can strengthen cyber defences, not just break them down; How AI can strengthen digital security | Google Keyword blog: https://blog.google/technology/safety-security/google-ai-cyber-defense-initiative/

[34] Google's Secure AI Framework (SAIF) - Google Safety Centre: https://safety.google/intl/en_in/safety/saif/

[35] How we're securing the AI frontier: https://blog.google/technology/safety-security/ai-security-frontier-strategy-tools/

[36] AI for Security | Google Cloud: https://cloud.google.com/security/ai

[37] $15 million to support hands-on cybersecurity education: https://blog.google/outreach-initiatives/google-org/cybersecurity-program/

[38] GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools | Google Cloud Blog: https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools

[39] SAIF.Google; Components of Generative AI Systems - SAIF: https://saif.google/focus-on-agents

[40] Announcing the CoSAI Principles for Secure-by-Design Agentic Systems: https://www.coalitionforsecureai.org/announcing-the-cosai-principles-for-secure-by-design-agentic-systems/

[41] Cloud CISO Perspectives: Our Big Sleep agent makes a big leap | Google Cloud Blog: https://cloud.google.com/blog/products/identity-security/cloud-ciso-perspectives-our-big-sleep-agent-makes-big-leap?e=48754805

[42] Introducing CodeMender: an AI agent for code security: https://deepmind.google/blog/introducing-codemender-an-ai-agent-for-code-security/

[43] Fog of war: how the Ukraine conflict transformed the cyber threat landscape: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

[44] Strengthening cyber defence: Google provides Ukrainian civil servants with 5,000 security keys to protect their accounts | Cabinet of Ministers of Ukraine: https://www.kmu.gov.ua/en/news/posyliuiemo-kiberzakhyst-google-nadaie-ukrainskym-derzhsluzhbovtsiam-5-tysiach-kliuchiv-bezpeky-dlia-zakhystu-oblikovykh-zapysiv

[45] Cloud CISO Perspectives: Why PQC is the next Y2K, and what you can do about it: https://cloud.google.com/blog/products/identity-security/cloud-ciso-perspectives-prepare-early-for-PQC-resilient-cryptographic-threats/

[46] Google Online Security Blog: Tracking the Cost of Quantum Factoring: https://security.googleblog.com/2025/05/tracking-cost-of-quantum-factori.html

[47] Google's Threat model for Post-Quantum Cryptography | Google Bughunters Blog: https://bughunters.google.com/blog/googles-threat-model-for-post-quantum-cryptography

[48] Summary of NATO's Rapid Adoption Action Plan | NATO Official text: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/summary-of-natos-rapid-adoption-action-plan

Google