

TRUST NO  
ONE,  
ESPECIALLY  
NOT US...  
BECAUSE WE  
KNOW THAT  
NOTHING IS  
TRULY  
SECURITY



#### Find more:

BOOSTY

SPONSR

TELEGRAM

#### Section: "Keypoints"

high-impact summaries of in-depth content, serving as a compacted edition of the other sections for quick, comprehensive overviews.

#### Section: "Unpacking"

tailored for critically reviews existing cyber content, highlighting benefits, drawbacks aspects.

#### Section: "Research"

original studies, experiments & in-depth investigations offering comprehensive reports and findings that advance the understanding of cybersecurity issues.

# SNARKY SECURITY

MONTHLY DIGEST. 2024 / 06

Welcome to the next edition of our Monthly Digest, your one-stop resource for staying informed on the most recent developments, insights, and best practices in the ever-evolving field of security. In this issue, we have curated a diverse collection of articles, news, and research findings tailored to both professionals and casual enthusiasts. Our digest aims to make our content both engaging and accessible. Happy reading!

Read more: [Boosty](#) | [Sponsr](#) | [TG](#)



SNARKY SECURITY



**NEWS**



## OIL & GAS INDUSTRY UNDER CYBER-ATTACKS & GAMIFICATION

LNG systems are vulnerable to cyber-attacks due to intrinsic system risks, which include remotely managed third-party systems and vulnerable onboard

technologies such as Programmable Logic Controllers (PLCs), Global Positioning System (GPS), and Automatic Identification System (AIS). These vulnerabilities could lead to overflowing fuel tanks, accidental release of LNG, and other risks that make LNG inaccessible or cause serious impacts when returned to its gaseous state

In mid-February 2022, hackers gained access to computers belonging to current and former employees at nearly two dozen major natural gas suppliers and exporters, including Chevron Corp., Cheniere Energy Inc. and Kinder Morgan Inc. These attacks targeted companies involved with the production of liquefied natural gas (LNG) and were the first stage in an effort to infiltrate an increasingly critical sector of the energy industry.

Additionally, the FBI has warned the energy sector of a likely increase in targeting by Chinese and Russian hackers due to changes in the global energy supply chain. The alert cites factors such as increased US exports of LNG and ongoing Western pressure on Russia's energy supply but does not mention any specific attacks on LNG tankers.

Chevron Corp., Cheniere Energy Inc., and Kinder Morgan Inc. are all headquartered in the United States. Chevron's global headquarters are located in San Ramon, California, Cheniere Energy's headquarters are in Houston, Texas, and Kinder Morgan's headquarters are in Houston, Texas

### **And now .... "We can't even build our own LNG tankers here in the United States"**

In a delightful twist of irony, it turns out that not a single shipyard in the United States is capable of building LNG tankers, as admitted by US Navy Secretary Carlos Del Toro in his testimony before Congress on Wednesday. "We've lost this art here in the United States. We can't even build our own LNG tankers here, in the United States," Del Toro told the US House Armed Services Committee. According to shipbuilding records, the last time a US shipyard produced an LNG tanker was in 1980.

This revelation is a perfect example of the gamification of consciousness, where people focus on developing certain technologies to a certain level, then become complacent and neglect continuous improvement, research, and development. After all, why bother, since we've already achieved what we need? We've been trained by computer games, where once something is invented, it doesn't need to be reinvented. We level up our technology, bask in the glory, and then move on.

But then reality comes knocking, with its annoying habit of not following the rules of a game. Technologies can be forgotten

and lost, progress can regress, and skilled workers can disperse and forget their skills. And if there's a 40-year gap between when a technology was last used and when it's decided to be revived, the principle of two dead generations comes into play. This principle states that 20-year-old engineers can be taught by 40-year-olds, but not by 60-year-olds. Even if someone who worked on technology in the 1980s is willing to teach, they may struggle to connect with the younger generation.

Cue the tears and cries of disbelief. "But I played on the computer, and it wasn't like this! It's too hard and confusing. Let's just pretend it's not true. After all, if the US could build a tanker or fly to the moon once, it must still be able to do so now. I believe it, and it's comforting and easy to believe it."



## OPEN SEASON ON CONFIDENTIALITY: BUNDESWEHR AND FEDERAL GOVERNMENT'S VIDEO CALL LINKS LEFT UNLOCKED AND ONLINE FOR ALL TO SEE

In a world where we expect military and government communications to be as secure as Fort Knox, it turns out that the Bundeswehr and the Federal Government were more akin to an open book at a yard sale (thanks to Webex): thousands of links to what were supposed to be confidential video meetings were just hanging out in the digital ether, accessible to anyone who could muster the Herculean effort of clicking a mouse.

And the response? The Bundeswehr assured that "unnoticed or unauthorized participation in video conferences" was as unlikely as finding a unicorn in your backyard, thus ensuring that no confidential content could have possibly leaked. Because, as we all know, if you can't see the problem, it doesn't exist.

Not forgetting the previous incidents that set the stage for this masterpiece of security theater. The Bundeswehr had already dazzled us with an eavesdropping scandal involving the Air Force, proving that when it comes to securing German military secrets, they're as reliable as a chocolate teapot.

### **Quick facts:**

- ◆ **Public Accessibility of Video Call Links:** Thousands of links to confidential video meetings were publicly accessible for months. This vulnerability allowed anyone to see who invited whom to a video call and when.

- ◆ **Platform Involved:** The video conferencing platform implicated in this security breach is Webex, a cloud service provided by Cisco. This platform was used not only by the Bundeswehr but also by all federal authorities, including for the first completely digital committee meeting of the Bundestag due to COVID-19 restrictions.

- ◆ **Response and Measures:** Upon discovery, the Bundeswehr disconnected its video conferencing system from

the internet. A spokesperson from the Cyber and Information Space Command confirmed that the vulnerability had been closed within 24 hours after it was reported. However, the Bundeswehr emphasized that "unnoticed or unauthorized participation in video conferences" was not possible due to this vulnerability, suggesting that no confidential content from the conferences could have leaked.

❖ **Criticism and Concerns:** The incident has drawn criticism regarding the handling of IT security within the Bundeswehr and the Federal Government. The Green Party's Konstantin von Notz criticized the "great carelessness" in the Federal Ministry of Defense, highlighting the importance of IT security checks, especially in handling sensitive security-political files and information.

❖ **Previous Incidents:** This is not the first time the Bundeswehr has faced security issues. In March of the same year, an eavesdropping scandal involving the Air Force was reported, where a conference call discussing the potential delivery of Taurus cruise missiles to Ukraine was leaked by Russia. This incident raised questions about the security of German military secrets and the effectiveness of the Bundeswehr's operational security (OPSEC).

❖ **Public and Political Reaction:** The security breach has sparked discussions on digital security and the need for stringent measures to protect sensitive information. It also reflects the ongoing challenges faced by government and military institutions in safeguarding their communications in the digital age.



### SANCTIONS & U.S.'S DIMINISHING ROLE AS A TECH LEADER

U.S. Department of the Treasury announcing a significant expansion of sanctions against Russia on May 1, 2024, ostensibly to curb Russia's technological capabilities. The stated reason for these sanctions is to degrade Russia's ability to sustain its war machine by targeting its military-industrial base and the networks that facilitate its access to crucial technology and equipment.

❖ **Broad Sanctions Imposed:** The Treasury has imposed sanctions on nearly 300 targets, including companies and individuals, to disrupt and degrade Russia's military-industrial base and its evasion networks that support the war effort.

❖ **Focus on Third-Country Support:** A significant aspect of these sanctions is the targeting of entities and individuals in third countries, notably in the People's Republic of China (PRC), that provide critical inputs to Russia's military-industrial base. This support is seen as enabling Russia to continue its war against Ukraine and is considered a threat to international security.

❖ **Sanctions on Military and Weapons Programs:** The sanctions specifically target Russia's military-industrial base and its chemical and biological weapons programs. This includes actions against companies and individuals that help Russia acquire key inputs for weapons or defense-related production.

❖ **Global Outreach and Guidance:** The Treasury and other U.S. government partners have issued extensive guidance and conducted outreach worldwide to educate and inform about the risks of doing business with Russia. This is part of a broader effort to disrupt Russia's military-industrial supply chains, regardless of their location.

❖ **Commitment to Unilateral Action:** The Treasury has expressed its commitment to taking unilateral action when necessary to disrupt Russia's acquisition of technology and equipment for its war efforts. This includes a readiness to impose sanctions on individuals and entities facilitating these acquisitions.

While the sanctions aim to prevent Russia from being a tech hegemon, they are catalyzing the development of Russia's technological independence and fostering stronger international alliances that could enhance its technological stature on the global stage. This outcome is quite the opposite of what the sanctions intended to achieve, highlighting the complex and often counterproductive nature of international economic policies in the geopolitical arena.

The reality emerges when this action is viewed as a response to the U.S.'s own technological stagnation or impotence. Despite being a global leader in technology historically, recent analyses and reports suggest that the U.S. is struggling to maintain its technological edge, particularly in comparison to rising powers like China and Russia. This decline in U.S. technological dominance might be seen as a driving factor behind the U.S.'s aggressive sanctions policy.

By imposing sanctions, the U.S. attempt to hinder the technological advancements of other nations, under the guise of national security, to compensate for its own inability to keep pace in the global tech race. This approach might be interpreted as an attempt to level the playing field by curbing the capabilities of potential competitors rather than through genuine security concerns.

Thus, the irony lies in that the U.S. is using sanctions not just as a tool of international policy but also as a crutch to support its own faltering technological sector, masking its vulnerabilities while trying to suppress the technological growth of other nations. This strategy could be seen as an admission of the U.S.'s diminishing role as a tech leader, cloaked in the rhetoric of security and defense.



## DEMOCRACY IN DISTRESS: EU'S CRUSADE AGAINST INFORMATION MANIPULATION

**EU is in full panic mode again**, trying to shield its precious democracy from the big bad wolves of foreign interference.

◆ **The Looming Threat:** Apparently, the next European elections are a «defining moment» for EU future. The EU is quaking in its boots over the possibility of foreign actors, especially Russia, meddling in the democratic process. The narrative is that these foreign entities are hell-bent on making Europe fail. How dramatic! The EU is just the star of the «Democracy» drama club!

◆ **and again, Russia is to blame:** Russia, with its arsenal of cheap AI tools and fake bot accounts, is supposedly flooding the EU's information space with deceptive content. They even have «Doppelganger» websites pretending to be authentic news outlets. The horror! These sites are picking on hot-button issues, adding scandalous and emotional content that spreads like wildfire online and has so far surpassed the EU in smear campaigns against European leaders that the EU has decided to flex its democratic inclusive muscles again.

◆ **Unreal Manipulations:** EU has seen that manipulation is not only happening online. The French authorities are shifting responsibility for organizing anti-Semitic actions in Paris to Russia to increase polarization according to the dogma «Everything good is the EU, and everything bad is, well, you get it»

### The EU's Grand Plan

◆ **Situational Awareness:** Keeping an eye on the threats.

◆ **Societal Resilience:** Building a society that can withstand these attacks.

◆ **Foreign Policy Instruments:** Using diplomatic tools to counteract interference.

◆ **Regulatory Tools:** Implementing laws like the Digital Services Act (DSA) to hold social media platforms accountable.

**Cooperation and Exposure:** The EU is working closely with Member States, the G7, academia, civil society, and tech companies to understand and fight foreign interference. They believe that exposing the tactics of these malign actors to the public is the best way to limit their impact. The EUvsDisinfo platform is their pride and joy, boasting the world's largest database of disinformation cases.

◆ **Personal Responsibility:** The EU also wants you, dear citizen, to take personal responsibility. They suggest you perform a «sanity check» on your information diet. Make sure it's diverse, healthy, and from reputable sources. Because, just like junk food, consuming junk information is bad for you, and you will be publicly (or not so publicly) punished for it in the name of democracy with centuries of crusading experience.

◆ **The Call to Vote:** Finally, the EU urges all citizens to go out and vote. Voting is portrayed as an act of defiance against authoritarian powers. If you don't vote, EU warns, others will decide for you. It is so authoritarian and ironic, but EU citizens must admit that they themselves decided to take such a step.

So, there you have it. The EU's frantic efforts to protect its democracy from the evil clutches of foreign interference. It's a mix of genuine concern and a touch of hysteria, wrapped up in a call for collective and personal action and seasoned with an infinity of responsibility not only for everyone.



## FBI, DATA LEAK AND DISCORD

The FBI is currently investigating another alleged data leak involving Discord, the popular communication platform widely used by gamers and various online communities. This probe follows recent incidents where large amounts of user data were reportedly compromised. The specifics of the data involved in this leak have not been fully disclosed, but the investigation aims to determine the extent of the breach and identify the perpetrators.

In 2022, the FBI investigated an Air Force intelligence analyst for leaking classified information in an anti-government group on Discord. The analyst, who was a member of the 381st Intelligence Squadron at Joint Base Elmendorf-Richardson (JBER) in Alaska, allegedly shared sensitive information with other members of the group, which had a focus on far-right and anti-government ideologies.

In response to the FBI's investigation, Discord has reiterated its commitment to user privacy and security. The company has reportedly taken additional measures to secure user data and prevent future breaches. Discord's spokesperson emphasized ongoing efforts to enhance security protocols in light of these repeated data leak incidents.

This incident has drawn attention from not only law enforcement but also data protection agencies. There is an ongoing discussion about the need for stricter data security laws and regulations, especially concerning platforms like Discord that handle significant amounts of sensitive user information.

The potential for stricter data security laws could have a significant impact on the way companies like Discord operate and the measures they are required to take to protect user data.



## U.S. AIR FORCE IS ASKING MONEY AGAIN

The U.S. Air Force has outlined its strategic vision for 2025, emphasizing an increase in flying operations and a move towards a more streamlined, "flat" workforce structure. This vision is part of its budget request for Fiscal Year 2025, where the Air Force is seeking

\$217.5 billion in funding. This request represents a significant investment in the future capabilities and readiness of the Air Force, aiming to adapt to the rapidly evolving nature of global threats and technological advancements.

**Increased Flying Operations:** The plan for increased flying operations is a response to the growing need for air superiority in an era where aerial threats and the strategic importance of air dominance are escalating. This includes not only traditional manned aircraft operations but also an increased reliance on unmanned aerial vehicles (UAVs) and remotely piloted aircraft (RPA), reflecting the ongoing shift towards more technologically advanced and versatile air combat capabilities.

**Flat Workforce Structure:** The move towards a "flat" workforce structure is indicative of the Air Force's commitment to becoming more agile and efficient. This approach aims to reduce bureaucratic layers, streamline decision-making processes, and foster a culture of innovation and rapid response to challenges. By flattening the organizational structure, the Air Force hopes to enhance its operational effectiveness and adaptability, ensuring that it can quickly respond to new threats and opportunities.

**Funding the Future:** The \$217.5 billion budget request for Fiscal Year 2025 is a clear indication of the Air Force's priorities and strategic direction. This funding is intended to support the dual goals of increasing flying operations and implementing a flat workforce structure, alongside other critical initiatives such as modernizing the nuclear triad, advancing space capabilities, and investing in cyber defense.

This budget request also reflects the broader strategic objectives of the Department of Defense, emphasizing readiness, modernization, and innovation to maintain the United States' military edge in an increasingly competitive global landscape.



## DELL HACKED

**Dell Announces Security Breach:** Dell Technologies has confirmed a significant data breach involving a database used to store information about customer purchases. The breach, which was disclosed on May 10, 2024, affected approximately 49 million

customers. The stolen data includes customer names, physical addresses, and details about Dell equipment but does not include sensitive information like payment details. Dell has initiated an investigation, notified law enforcement, and hired a third-party forensic firm to further investigate the incident.

**Details of the Breach:** The breach was executed by exploiting an unsecured API attached to a partner portal. The threat actor, known as Menelik, claimed to have scraped information of 49 million customer records using this method. The data includes a wide range of hardware details, such as service tags, item descriptions, order dates, and warranty details. Dell was reportedly notified about the vulnerability by the threat actor before the data was put up for sale on a hacking forum, but the breach was not contained until ~ two weeks later.

**Customer Notification and Response:** Dell has sent out notifications to its customers warning them about the breach. The company has downplayed the significance of the stolen data, stating that it does not include financial or highly sensitive customer information. However, Dell has advised customers to be vigilant against potential tech support scams that could use the stolen hardware details to impersonate Dell support technicians.

**Legal and Regulatory Implications:** This incident adds to a series of data breaches that Dell has experienced over the years, raising concerns about the company's data protection measures and cybersecurity practices. Previous breaches have led to class-action lawsuits and investigations by privacy commissioners, highlighting the legal and regulatory implications for Dell.

**Cybersecurity Measures and Recommendations:** In response to the breach, Dell has emphasized its commitment to cybersecurity, offering various services and solutions aimed at enhancing IT security and cyber resiliency. The company provides a range of products and advisory services designed to improve threat detection, threat response, and cyber recovery capabilities.



## ASCENSION HACKED

Ascension, one of the largest non-profit Catholic health systems in the United States, has recently suffered a significant cyberattack impacting its operations across 140 hospitals in 19 states. The attack was detected on Wednesday, and it has caused widespread disruptions to clinical operations and patient care.

**Overview of the Cyberattack:** The cyberattack on Ascension was first noticed due to "unusual activity" on select technology systems. It has led to the shutdown of electronic health records, patient communication portals like MyChart, and various systems used for ordering tests, procedures, and medications. This disruption has forced the healthcare provider to revert to manual systems for patient care, reminiscent of pre-digital times.

❖ **Impact on Patient Care:** The cyberattack has severely impacted patient care across Ascension's network. Ambulances have been diverted, and non-emergent elective procedures have been temporarily suspended to prioritize urgent care. Patients have been advised to bring detailed notes about their symptoms and a list of medications to their appointments.

❖ **Root cause:** The type of cyberattack has been identified as a ransomware attack, specifically linked to the Black Basta ransomware group. Black Basta ransomware typically infiltrates networks through methods such as phishing emails, exploiting software vulnerabilities, or using compromised creds.

❖ **RaaS:** Black Basta is a ransomware-as-a-service (RaaS) group that emerged in early 2022 and has been linked to several high-profile attacks. The group is known for its double extortion tactics, which involve encrypting the victim's data and threatening to release it publicly if the ransom is not paid. This group has targeted various sectors, including healthcare, indicating a pattern of attacks against organizations with critical infrastructure.

❖ **Entry Points:** Entry point or vulnerability exploited by the attackers includes initial access through phishing, exploitation of public-facing applications, the use of previously compromised credentials to gain deeper access to the network.

❖ **Broader Implications:** This incident is part of a larger trend of increasing cyberattacks on healthcare systems, which are particularly vulnerable due to the critical nature of their services and the valuable data they hold. The attack on Ascension highlights the ongoing challenges and the need for robust cybersecurity measures in the healthcare sector.

❖ **Response to the Cyberattack:** Ascension has engaged Mandiant, a cybersecurity firm and Google subsidiary, to assist in the investigation and remediation process. The focus is on investigating the breach, containing it, and restoring the affected systems. However, there is currently no timeline for when systems will be fully operational again.



## WHY SPIES NEED AI: BECAUSE GUESSWORK IS OVERRATED

Microsoft has developed a [generative AI model](#) for U.S. intelligence agencies to analyze top-secret information.

❖ **Development and Purpose:** Microsoft has developed a generative AI model based on GPT-4 technology specifically for U.S. intelligence agencies to analyze top-secret information. The AI model operates in an "air-gapped" environment, completely isolated from the internet, ensuring secure processing of classified data.

❖ **Security and Isolation:** This is the first instance of a large language model functioning independently of the internet, addressing major security concerns associated with generative AI. The model is accessible only through a special network

exclusive to the U.S. government, preventing any external data breaches or hacking attempts.

❖ **Development Timeline and Effort:** The project took 18 months to develop, involving the modification of an AI supercomputer in Iowa. The model is currently undergoing testing and accreditation by the intelligence community.

❖ **Operational Status:** The AI model has been operational for less than a week and is being used to answer queries from approximately 10,000 members of the U.S. intelligence community.

❖ **Strategic Importance:** The development is seen as a significant advantage for the U.S. intelligence community, potentially giving the U.S. a lead in the race to integrate generative AI into intelligence operations.

## Intelligence and National Security

❖ **Enhanced Analysis:** Provides U.S. intelligence agencies with a powerful tool to process and analyze classified data more efficiently and comprehensively, potentially improving national security and decision-making.

❖ **Competitive Edge:** Positions the U.S. ahead of other countries in the use of generative AI for intelligence purposes, as highlighted by CIA officials.

## Cybersecurity and Data Protection

❖ **Assurance:** Air-gapped environment ensures that classified information remains secure, setting a new standard for handling sensitive data with AI.

❖ **Precedent for Secure AI:** Demonstrates the feasibility of developing secure, isolated AI systems, which could influence future AI deployments in other sensitive sectors.

## Technology and Innovation

❖ **Groundbreaking Achievement:** Marks a significant milestone in AI development, showcasing the ability to create large language models that operate independently of the internet.

❖ **Future Developments:** Encourages further advancements in secure AI technologies, potentially leading to new applications in various industries such as healthcare, finance, and critical infrastructure.

## Government and Public Sector

❖ **Government Commitment:** Reflects the U.S. government's dedication to leveraging advanced AI technology for national security and intelligence.

❖ **Broader Adoption:** May spur increased investment and adoption of AI technologies within the public sector, particularly for applications involving sensitive or classified data.



## EUROPOL HACKED BY INTELBROKER

The breach at Europol by the hacker known as IntelBroker, which occurred on May 10, 2024, has resulted in a significant data breach exposing highly sensitive and classified information. This incident has raised serious concerns about the security measures at Europol and the potential exploitation of the exposed data by other malicious actors.

◆ **Details of the Breach:** IntelBroker, a key member of the CyberNiggers threat group, has been involved in various high-profile cyber incidents, including earlier breaches at HSBC and Zscaler. The compromised data from the Europol breach includes sensitive materials such as alliance employee information, For Official Use Only (FOUO) source code, PDFs, documents for reconnaissance, and operational guidelines. This breach poses immediate security risks to Europol's operations and highlights the vulnerabilities within Europol's cybersecurity infrastructure.

◆ **Affected Europol Entities:** The breach has impacted several entities within Europol, including the CCSE, EC3, Europol Platform for Experts, Law Enforcement Forum, and SIRIUS. The infiltration of these entities could disrupt ongoing investigations and compromise sensitive intelligence shared among international law enforcement agencies.

◆ **Europol's Response:** As of the latest updates, Europol has not made any public announcements regarding the breach. However, they have confirmed a separate incident involving their Europol Platform for Experts (EPE) portal, stating that no operational data was stolen in that specific incident.

◆ **Broader Implications:** This incident underscores the need for enhanced security measures to safeguard against future incidents. The breach not only threatens the integrity of Europol's operations but also has broader implications for international law enforcement cooperation and data security.

◆ **Monitoring and Future Actions:** To track activities of threat actors like IntelBroker, monitoring dark web sources such as hacker forums and private Telegram channels is crucial. These platforms often serve as venues for cyber threats to originate and proliferate.

◆ **Root of Cause:** The breach of Europol's Europol Platform for Experts (EPE) portal by IntelBroker was primarily facilitated through the exploitation of vulnerabilities within the system. IntelBroker's method typically involves identifying and exploiting these vulnerabilities to gain unauthorized access to systems. In the case of the EPE breach, the hacker managed to access sensitive data, including For Official Use Only (FOUO) documents and classified data, which were then claimed to be up for sale. This incident highlights the critical need for robust cybersecurity measures and regular system updates to patch any vulnerabilities that could be exploited by malicious actors.



## ZSCALER HACKED BY INTELBROKER

IntelBroker claims to have breached Zscaler and sold access to its systems, Zscaler maintains that there has been no compromise of its main environments and that only an isolated test environment was affected. The situation continues to develop as investigations proceed.

### IntelBroker's Claims:

- ◆ IntelBroker, a known threat actor, claimed to have breached Zscaler's systems.
- ◆ The actor allegedly accessed confidential logs packed with credentials, including SMTP access, PAuth access, and SSL passkeys and certificates.
- ◆ IntelBroker offered to sell this access for \$20,000 in cryptocurrency.

### Zscaler's Response and Findings:

- ◆ Zscaler has consistently denied any impact or compromise to its customer, production, and corporate environments.
- ◆ The company acknowledged the exposure of an isolated test environment on a single server, which was not connected to Zscaler's infrastructure or hosting any customer data.
- ◆ This test environment was exposed to the internet and subsequently taken offline for forensic analysis.

### Investigative Measures:

- ◆ Zscaler engaged a reputable incident response firm to conduct an independent investigation.
- ◆ The company has been providing regular updates, asserting the security of its main operational environments.
- ◆ Zscaler emphasized that the exposure of the test environment does not affect the security of its primary systems and data.

### IntelBroker's Background and Credibility:

- ◆ IntelBroker has a history of making bold claims about breaches, including previous allegations against high-profile targets like the US State Department and various corporate entities.
- ◆ Threat actor is also known for previous breaches involving companies like PandaBuy and HomeDepot, claims of stealing data from General Electric.

### Root Cause of the Alleged Hack:

- ◆ The root cause, as claimed by IntelBroker, centers on the exploitation of the isolated test environment that was inadvertently exposed to the internet.

➡ Zscaler's investigation discovered only this exposure, which did not involve any customer data or connection to its main infrastructure.

#### Contradictions and Ongoing Developments:

➡ IntelBroker's assertion that the access sold was not to a testing environment contradicts Zscaler's findings.

➡ Zscaler maintains that there has been no compromise of its main systems and has taken steps to ensure the continued security of its environments.



### AI FOR CHRONICALLY LAZY: MASTERING ART OF DOING NOTHING WITH GEMINI

The updates to [Gemini](#) and Gemma models significantly enhance their technical capabilities and broaden their impact across various industries, driving innovation and efficiency while promoting responsible AI development.

#### Gemini 1.5 Pro and 1.5 Flash Models:

➡ **Gemini 1.5 Pro:** Enhanced for general performance across tasks like translation, coding, reasoning, and more. It now supports a 2 million token context window, multimodal inputs (text, images, audio, video), and improved control over responses for specific use cases.

➡ **Gemini 1.5 Flash:** A smaller, faster model optimized for high-frequency tasks, available with a 1 million token context window.

#### Gemma Models:

➡ **Gemma 2:** Built for industry-leading performance with a 27B parameter instance, optimized for GPUs or a single TPU host. It includes new architecture for breakthrough performance and efficiency.

➡ **PaliGemma:** A vision-language model optimized for image captioning and visual Q&A tasks.

#### New API Features:

➡ **Video Frame Extraction:** Allows developers to extract frames from videos for analysis.

➡ **Parallel Function Calling:** Enables returning more than one function call at a time.

➡ **Context Caching:** Reduces the need to resend large files, making long contexts more affordable.

#### Developer Tools and Integration:

➡ **Google AI Studio and Vertex AI:** Enhanced with new features like context caching and higher rate limits for pay-as-you-go services.

➡ **Integration with Popular Frameworks:** Support for JAX, PyTorch, TensorFlow, and tools like Hugging Face, NVIDIA NeMo, and TensorRT-LLM.

#### Impact on Industries

##### Software Development:

➡ **Enhanced Productivity:** Integration of Gemini models in tools like Android Studio, Firebase, and VSCode helps developers build high-quality apps with AI assistance, improving productivity and efficiency.

➡ **AI-Powered Features:** New features like parallel function calling and video frame extraction streamline workflows and optimize AI-powered applications.

##### Enterprise and Business Applications:

➡ **AI Integration in Workspace:** Gemini models are embedded in Google Workspace apps (Gmail, Docs, Drive, Slides, Sheets), enhancing functionalities like email summarization, Q&A, and smart replies.

➡ **Custom AI Solutions:** Businesses can leverage Gemma models for tailored AI solutions, driving efficiency and innovation across various sectors.

##### Research and Development:

➡ **Open-Source Innovation:** Gemma's open-source nature democratizes access to advanced AI technologies, fostering collaboration and rapid advancements in AI research.

➡ **Responsible AI Development:** Tools like the Responsible Generative AI Toolkit ensure safe and reliable AI applications, promoting ethical AI development.

##### Multimodal Applications:

➡ **Vision-Language Tasks:** PaliGemma's capabilities in image captioning and visual Q&A open new possibilities for applications in fields like healthcare, education, and media.

➡ **Multimodal Reasoning:** Gemini models' ability to handle text, images, audio, and video inputs enhances their applicability in diverse scenarios, from content creation to data analysis.



### THE U.S. SANCTIONS SPREE: A MASTERCLASS IN GLOBAL BULLYING

The recent [actions](#) by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) on June 12, 2024, reflect a desperate attempt by a once-dominant global power to maintain its waning influence. U.S. is in a manic panic, flailing about with new sanctions in a futile attempt to regain control and influence. It's a classic case of a lost hegemon trying to assert dominance through increasingly desperate measures.

❖ **Russia-related Designations:** The U.S. has added more names to its ever-growing list of sanctioned Russian entities and individuals. Because, you know, if the first 4,000 sanctions didn't work, surely the next 300 will do the trick.

❖ **Targeting Chinese Firms:** The U.S. is now going after Chinese companies that dare to do business with Russia. It's almost as if the U.S. believes that bullying other countries into compliance will somehow restore its lost hegemony.

❖ **Secondary Sanctions:** Foreign financial institutions are now at risk of sanctions if they deal with any of the newly sanctioned Russian entities. Because nothing says «global leadership» like threatening the entire world's banking system.

❖ **Expanding Definitions:** The Treasury has broadened the definition of Russia's «military-industrial base» to include just about anyone and anything remotely connected to Russia. It's a classic move: when in doubt, just make the net wider.

❖ **Restricting IT Services:** The U.S. is restricting the supply of IT services and software to Russia. Because clearly, cutting off access to Microsoft Office will bring the Russian war machine to its knees.

❖ **Global Networks:** The sanctions also target transnational networks in countries like China, Turkey, and the UAE. It's almost as if the U.S. is trying to pick a fight with half the world at once.

❖ **G7 Summit:** These actions come just in time for the G7 summit, where world leaders will undoubtedly pat themselves on the back for their «tough stance» on Russia. Meanwhile, Russia continues to adapt and find new ways to circumvent these measures.

#### Affected Industries:

❖ **Financial Services:** Multiple documents highlight sanctions and exemptions related to financial transactions and services.

❖ **Cyber Operations:** Entities involved in cyber activities are specifically targeted.

❖ **Humanitarian Aid:** Exemptions are provided for transactions related to humanitarian aid.

❖ **Energy Sector:** Sanctions target entities in the energy industry.

❖ **Defense Sector:** Entities in the defense industry are affected by the sanctions.

❖ **Maritime Industry:** Vessels added to the SDN List indicate that the maritime industry is also affected. This includes shipping companies and operators of vessels that are involved in activities supporting sanctioned entities or individuals.

#### [Full list](#)

These documents collectively provide a comprehensive overview of the recent actions taken by OFAC in relation to Russia, including designations, general licenses, determinations, and guidance on compliance.

#### [Document 932921](#)

❖ **Russia-related Designations:** This document lists individuals and entities designated under the Russia-related sanctions program.

❖ **Sanctions Criteria:** It outlines the criteria for these designations, including involvement in destabilizing activities, cyber operations, and support for the Russian government.

#### [Document 932926](#)

❖ **General Licenses:** This document details new general licenses issued by OFAC. These licenses provide exemptions for certain transactions and activities that would otherwise be prohibited under the sanctions.

❖ **Specific Transactions:** It specifies the types of transactions allowed under these licenses, such as humanitarian aid and certain financial services.

#### [Document 932931](#)

❖ **Determination on Russian Financial Sector:** This document contains a determination related to the Russian financial sector, outlining specific actions and criteria subject to sanctions.

❖ **Implementation Guidance:** It provides guidance on how these determinations will be implemented and enforced.

#### [Document 932936](#)

❖ **Updated FAQs:** This document includes updated Frequently Asked Questions (FAQs) to provide additional guidance on the implementation of Russia-related sanctions.

❖ **Compliance Requirements:** It addresses common queries and clarifies compliance requirements for individuals and businesses affected by the sanctions.

#### [Document 932941](#)

❖ **Additional Designations:** This document lists additional individuals and entities designated under the Russia-related sanctions program.

❖ **Rationale for Designations:** It explains the rationale behind these designations, focusing on their roles in activities.

#### [Document 932946](#)

❖ **Sectoral Sanctions:** This document outlines sectoral sanctions targeting specific sectors of the Russian economy, such as energy, finance, and defense.

❖ **Prohibited Activities:** It details the specific activities and transactions that are prohibited under these sectoral sanctions.



Antarctica is driven by various strategic, security, and environmental factors

## China

❖ **BeiDou Navigation Satellite System (BDS):** China uses its own BeiDou system, which has been recognized as a global standard for commercial aviation and other applications. It provides both civilian and military services and is part of China's strategy to achieve technological self-sufficiency and reduce dependency on the U.S. GPS.

❖ **Obfuscation Algorithm:** The GCJ-02 system, also known as "Mars Coordinates," uses an obfuscation algorithm that introduces random offsets to latitude and longitude coordinates. This is intended to prevent accurate mapping by foreign entities, which could be used for military or intelligence purposes.

❖ **Legal Framework:** The Surveying and Mapping Law of the People's Republic of China mandates that all geographic data must be processed using the GCJ-02 system. Unauthorized mapping or surveying activities are strictly prohibited and can result in severe penalties, including fines and legal action. Companies providing location-based services in China must obtain authorization from the Chinese government and use the GCJ-02 system. This includes purchasing a "shift correction" algorithm to align GPS coordinates correctly on maps.

❖ **Cold War Era:** The use of a different coordinate system dates back to the Cold War era, aimed at frustrating foreign intelligence efforts. The GCJ-02 system continues to serve this purpose by ensuring that geographic data within China cannot be easily used for unauthorized purposes.

❖ **Daily Navigation:** For users in China, this means that GPS devices and applications may show their location inaccurately on maps unless they use local services like Baidu Maps, which also employs an additional layer of obfuscation called BD-09.

❖ **Device Restrictions:** Many GPS-enabled devices, including cameras and smartphones, have restrictions or modifications to comply with Chinese laws. This can include disabling geotagging features or using modified GPS chips that align with GCJ-02.

## India

❖ **Indian Regional Navigation Satellite System (IRNSS):** India has developed its own regional navigation system, known as NavIC (Navigation with Indian Constellation), to reduce dependency on foreign GPS systems like the U.S. GPS. This system ensures regional self-reliance,

enhances positioning accuracy, and provides strategic advantages, especially for military operations.

❖ **Strategic Autonomy:** The development of NavIC was partly motivated by the denial of GPS data by the U.S. during the Kargil War in 1999. NavIC provides India with an independent and reliable navigation system that can be used for both civilian and military purposes.

## Israel and Palestine

❖ **GPS Jamming and Spoofing:** Israel uses GPS jamming and spoofing as defensive measures to protect against potential attacks from adversaries like Hezbollah and Iran. This jamming can disrupt enemy navigation systems and precision-guided weapons, but it also affects civilian GPS services, causing inaccuracies in location data for apps like Google Maps and Uber.

❖ **Security Measures:** The use of GPS jamming is primarily for defensive purposes, to prevent the use of GPS-guided munitions by adversaries. This has led to significant disruptions in civilian navigation and communication systems in the region.

## North Korea

❖ **GLONASS and BeiDou:** North Korea avoids using the U.S. GPS due to concerns about potential disruption by the U.S. military. Instead, it uses Russia's GLONASS and China's BeiDou systems for its navigation needs, including missile tests.

❖ **GPS Jamming:** North Korea has been known to jam GPS signals, particularly in the Yellow Sea, as a means of disrupting South Korean and allied military operations. This jamming can affect civilian aircraft and ships, leading to navigation challenges.

❖ **Limited Access:** The general population in North Korea has limited access to GPS-enabled devices and the internet, making the impact of GPS jamming more significant for external entities rather than for daily civilian use within the country.

## Westchester County, New York

❖ **Security-Related Blurring:** Certain locations in Westchester County are intentionally blurred on Google Maps to prevent potential terrorist attacks. This measure is taken to protect sensitive sites and infrastructure, but it can hinder accurate navigation for residents and visitors.

❖ **Impact on Navigation:** The blurring of maps can make it difficult for users to find specific locations, affecting daily navigation and potentially leading to confusion.

## Antarctica

❖ **GPS:** Antarctica primarily relies on the U.S. GPS for navigation and scientific research. The harsh environment and dynamic ice landscape present unique challenges, but GPS remains the most accurate and reliable system available for this region.

❖ **Common Mode Errors (CME):** Antarctica does not use a different GPS standard, but the region faces unique challenges due to common mode errors in GPS coordinate time-

series. These errors are caused by environmental factors and systematic issues, affecting the accuracy of GPS measurements used for scientific research and navigation.

❖ **Harsh Environment:** The extreme conditions and vast, featureless ice landscapes make high-resolution mapping difficult. Specialized techniques and equipment are required to achieve accurate GPS data, which is crucial for scientific studies and logistical operations.

## Impact

Inaccurate mapping systems can significantly impact daily navigation in various regions around the world, including China, India, Israel and Palestine, North Korea, Westchester County in New York, and Antarctica.

### China

#### Misalignment of Maps and GPS Data

❖ **Offset Issues:** The GCJ-02 system introduces random offsets to latitude and longitude, ranging from 50 to 500 meters. This results in GPS coordinates (based on the global WGS-84 system) not aligning correctly with Chinese maps, which use GCJ-02.

❖ **Practical Impact:** For users, this means that GPS devices and applications may show their location inaccurately on maps. For example, a GPS coordinate might place a user in a different part of a city than their actual location.

#### Challenges for Foreign Mapping Services

❖ **Google Maps:** Google Maps in China must use the GCJ-02 system for street maps but uses WGS-84 for satellite imagery, causing visible misalignments between the two. This discrepancy can make navigation difficult for users relying on Google Maps.

❖ **Other Services:** Similar issues affect other foreign mapping services, which must either comply with GCJ-02 or face inaccuracies. Unauthorized mapping or attempts to correct the offsets without approval are illegal.

#### Local Solutions and Workarounds

❖ **Chinese Apps:** Local apps like Baidu Maps and WeChat use the GCJ-02 system and often provide more accurate navigation within China. Baidu Maps even uses an additional layer of obfuscation called BD-09.

❖ **Conversion Tools:** Several open-source projects and tools exist to convert between GCJ-02 and WGS-84 coordinates, helping developers and users mitigate some of the navigation issues.

#### Legal and Security Implications

❖ **Regulations:** The Chinese government enforces strict regulations on geographic data to protect national security. Unauthorized mapping activities can result in severe penalties, including fines and legal action.

❖ **Device Restrictions:** Many GPS-enabled devices, including cameras and smartphones, have restrictions or modifications to comply with Chinese laws. This can include

disabling geotagging features or using modified GPS chips that align with GCJ-02.

### India

❖ **Routing Issues:** Google Maps in India often suggests inefficient or incorrect routes, such as diverting users through small villages or bad road patches when better roads are available. This can lead to longer travel times and confusion, especially for first-time users.

❖ **Residential Colonies:** The app sometimes directs users through residential colonies, which may have restricted access or closed gates, causing further navigation problems.

❖ **Taxi Services:** Users of taxi-hailing apps like Uber and OLA frequently experience inaccuracies in the location of cars and their own position, necessitating phone calls to drivers for precise directions.

### Israel and Palestine

❖ **Biased Routing:** Google Maps prioritizes routes for Israeli citizens, often ignoring the segregated road system and checkpoints that affect Palestinians. This can result in suggested routes that are illegal or dangerous for Palestinians to use.

❖ **Omission of Palestinian Localities:** Many Palestinian villages and localities are either misrepresented or omitted from maps, which can alienate Palestinians from their homeland and complicate navigation within these areas.

❖ **Political Bias:** Maps often reflect political biases, such as labeling Israeli settlements clearly while Palestinian areas are left blank or inaccurately labeled. This affects the usability of maps for Palestinians and can lead to significant navigation challenges.

### North Korea

❖ **Limited Data:** While Google Maps has started to include more detailed information about North Korea, the data is still limited and often outdated. This makes it difficult for users to navigate accurately within the country.

❖ **Restricted Access:** The majority of North Koreans do not have access to the internet or GPS-enabled devices, rendering the available mapping data largely useless for local navigation.

### Westchester County, New York

❖ **Blurring for Security:** Certain locations in Westchester County are intentionally blurred on Google Maps to prevent potential terrorist attacks. This can hinder accurate navigation and make it difficult for users to find specific locations.

❖ **General Inaccuracies:** The map data may not always reflect the most current or precise information, which can affect navigation for residents and visitors alike.

### Antarctica

❖ **Low-Resolution Imagery:** Large areas of Antarctica are shown in low resolution or are blurred due to the featureless ice and snow, making high-resolution imaging difficult and largely unnecessary.

❖ **Survey Challenges:** Accurate mapping in Antarctica requires specialized equipment and techniques, such as Differential GPS Surveying, to minimize errors. This can be logistically challenging and expensive, affecting the availability of accurate maps for navigation.

❖ **Limited Use:** The practical need for detailed maps in Antarctica is limited to scientific and logistical operations, rather than daily navigation for the public.

### Benefits of Inaccurate Maps for Specific Countries

#### China

❖ **National Security:** The primary benefit of using the GCJ-02 coordinate system, which introduces intentional offsets, is to protect national security. By obfuscating geographic data, China prevents foreign entities from using accurate maps for military or intelligence purposes.

❖ **Economic Protectionism:** The policy also supports local mapping companies by limiting competition from foreign mapping services, ensuring that only authorized providers can offer accurate maps within China.

#### India

❖ **Territorial Integrity:** India enforces strict regulations on maps to ensure that its territorial claims, especially in disputed regions like Kashmir and Arunachal Pradesh, are accurately represented. This helps maintain national sovereignty and supports India's geopolitical stance.

❖ **Strategic Autonomy:** By developing its own regional navigation system (NavIC), India reduces dependency on foreign GPS systems, enhancing both civilian and military navigation capabilities.

#### Israel and Palestine

❖ **Security Measures:** Israel uses GPS jamming and spoofing to protect against potential attacks from adversaries. This defensive measure disrupts enemy navigation systems and precision-guided weapons, enhancing national security.

❖ **Political Narratives:** Both Israel and Palestine use maps to support their respective territorial claims. Inaccurate or biased maps can influence public perception and international opinion, which is crucial in the ongoing conflict.

#### North Korea

❖ **Military Defense:** North Korea employs GPS jamming to disrupt foreign military operations, particularly those of

South Korea and its allies. This measure complicates navigation for adversaries, providing a strategic defense advantage.

❖ **Controlled Information:** The limited and outdated mapping data available within North Korea helps the regime maintain control over information and restricts the population's access to external geographic data.

#### Westchester County, New York

❖ **Security Concerns:** Certain locations in Westchester County are intentionally blurred on maps to prevent potential terrorist attacks. This measure protects sensitive sites and infrastructure from being targeted.

#### Antarctica

❖ **Environmental Protection:** Inaccurate or less detailed maps can help protect sensitive environmental areas by limiting human activity and reducing the risk of exploitation or damage.

❖ **Scientific Research:** The dynamic and harsh environment of Antarctica makes accurate mapping challenging. However, the focus on improving mapping accuracy supports scientific research and environmental management.

#### Drawbacks for Other Countries

❖ **Navigation Challenges:** Inaccurate maps can lead to significant navigation issues for travelers, businesses, and emergency services. This can result in inefficiencies, increased travel times, and potential safety hazards.

❖ **Economic Impact:** Businesses that rely on accurate geographic data, such as logistics and delivery services, can face operational challenges and increased costs due to map inaccuracies.

❖ **Geopolitical Tensions:** Inaccurate maps can exacerbate territorial disputes and contribute to geopolitical tensions. Misrepresentation of borders and territories can lead to conflicts and diplomatic issues.

❖ **Scientific Limitations:** In regions like Antarctica, inaccurate maps hinder scientific research and environmental management. Accurate geographic data is crucial for studying climate change, managing natural resources, and protecting ecosystems.

❖ **Public Misinformation:** Inaccurate maps can mislead the public and perpetuate misinformation. This can affect education, public opinion, and policymaking, leading to a less informed society.

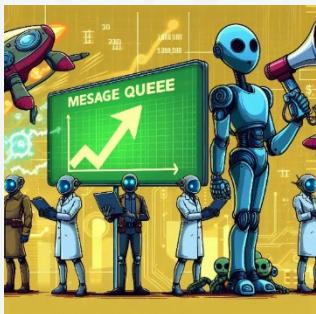
Read more: [Boosty](#) | [Sponsr](#) | [TG](#)



STARRY SECURITY

# CONTENTS





## MQ MARKET INSIGHTS. SIMPLE SOLUTIONS ARE JUST TOO CHEAP, SPENDING MORE IS ALWAYS BETTER

We embark on a thrilling journey through the labyrinthine world of Message Queue Brokers, dissecting their market with the precision of a surgeon and the enthusiasm of a caffeine-fueled techie. This analysis will cover a myriad of aspects, each more riveting than the last, including diving into market growth, like scalability, performance, and the ever-elusive interoperability. It's like a soap opera, but with more data and fewer dramatic pauses. This analysis is a goldmine for security professionals and other specialists across various industries, offering insights into the secure and efficient management of distributed systems. Whether you're in IT, forensics, or just a curious bystander, this document will equip you with the knowledge to make informed decisions and enhance your operational capabilities. So, buckle up and enjoy the ride through the fascinating world of message brokers!



## MARITIME SECURITY

In the grand theater of global trade, seaports are the unsung heroes, until, of course, they fall victim to cyber-physical attacks, and suddenly everyone's a critic about how vulnerable they are. This document takes a magnifying glass to the economic chaos that ensues when hackers decide to play Battleship with real ports. We're taking a deep dive into the world of econometric losses, where the ripple effects are not just a fancy term but a harsh reality for industries far and wide. It's a tale of direct economic hits, the domino effect on sectors you didn't even know cared about ports, and the glaring security gaps that let the bad guys waltz right in. A high-quality summary is a treasure trove for security buffs, IT gurus, and policy wonks, providing a map to navigate the stormy seas of potential disruptions. The analysis is like a lighthouse guiding the development of cyber resilience strategies that are as robust as the hull of a battleship. For those in the trenches of critical infrastructure, these insights are the ammunition needed to fortify against the cyber onslaught, ensuring economic stability doesn't go down with the ship. So, while the paper might not make seaports any less of a target, it certainly arms the good guys with knowledge, because knowing is half the battle, and in this case, it just might save the global economy from a virtual torpedo.



intrusion sets, and from 0day exploits to security bypassing techniques.

Most of them have been involved in nation-state offensive cyber operations, which is just a fancy way of saying they help governments spy on each other and have turned paranoia into profit, and all it took was a little creativity and a flexible moral compass

So, if you ever feel like your privacy is being respected a little too much, just remember that there's a whole industry out there working tirelessly to ensure that your secrets are as private as a tweet on a billboard. And to all the offensive security private companies out there, we salute you. Without your tireless efforts, the internet would be a much less interesting place



## CHOOSING SECURE AND VERIFIABLE TECHNOLOGIES

Another document on cybersecurity practices—because what the world needs is more guidelines, right? "Choosing Secure and Verifiable Technologies" rolls out the red carpet for organizations that are knee-deep in digital products and services but can't seem to figure out the whole security thing on their own. It's packed with everything from the joys of navigating manufacturer transparency (because they're always so forthcoming) to the rollercoaster ride of supply chain risks (spoiler alert: it's a doozy!).

And who gets to enjoy this page-turner? Not just anyone! We're talking high-level execs who need to justify their cybersecurity budget, IT managers who live to decode another risk assessment matrix, and procurement specialists who get giddy over compliance checklists. But let's not forget the manufacturers—they're in for a treat learning about all the hoops they'll need to jump through to prove their tech is as secure as a duck in a shark cage.

So buckle up, dear reader. Whether you're looking to safeguard national security or just keep your company's data from becoming the next headline, this document promises to guide you through the cybersecurity jungle with the finesse of a machete-wielding guide. Just remember, it's not a checklist—it's a way of life.

## OFFENSIVE COMPANIES

Ah, the shadowy world of offensive security private companies, where the line between white hats and black hats is as clear swing state.

These enterprising companies peddle in the digital dark arts, offering everything from software implants to intrusion sets, and from 0day exploits to security bypassing techniques.

intrusion sets, and from 0day exploits to security bypassing techniques.

Most of them have been involved in nation-state offensive cyber operations, which is just a fancy way of saying they help governments spy on each other and have turned paranoia into profit, and all it took was a little creativity and a flexible moral compass

So, if you ever feel like your privacy is being respected a little too much, just remember that there's a whole industry out there working tirelessly to ensure that your secrets are as private as a tweet on a billboard. And to all the offensive security private companies out there, we salute you. Without your tireless efforts, the internet would be a much less interesting place



## CHOOSING SECURE AND VERIFIABLE TECHNOLOGIES

Another document on cybersecurity practices—because what the world needs is more guidelines, right? "Choosing Secure and Verifiable Technologies" rolls out the red carpet for organizations that are knee-deep in digital products and services but can't seem to figure out the whole security thing on their own. It's packed with everything from the joys of navigating manufacturer transparency (because they're always so forthcoming) to the rollercoaster ride of supply chain risks (spoiler alert: it's a doozy!).

And who gets to enjoy this page-turner? Not just anyone! We're talking high-level execs who need to justify their cybersecurity budget, IT managers who live to decode another risk assessment matrix, and procurement specialists who get giddy over compliance checklists. But let's not forget the manufacturers—they're in for a treat learning about all the hoops they'll need to jump through to prove their tech is as secure as a duck in a shark cage.

So buckle up, dear reader. Whether you're looking to safeguard national security or just keep your company's data from becoming the next headline, this document promises to guide you through the cybersecurity jungle with the finesse of a machete-wielding guide. Just remember, it's not a checklist—it's a way of life.



## CYBERSECURITY & ANTARCTICA

In a stunning display of indifference that barely registered a blip on the global radar, the US decided to hit the pause button on its scientific endeavors in the frosty expanse of Antarctica. Yes, in a move that screams "we're broke," both the vast, mysterious continent and its surrounding icy waters have been left to fend for themselves.

In a revelation that shocked precisely zero people, the U.S. National Science Foundation (NSF) declared in April that it was too cash-strapped to bother with new field research this season. Why? Because upgrading the McMurdo Station is apparently as complex as rocket science. The NSF, along with the U.S. Coast Guard, also took this opportunity to announce cuts that essentially put America's scientific street cred on thin ice for the foreseeable future. Specifically, the NSF decided that Laurence M. Gould was no longer worth the lease, and why stop there? They figured operating just one research vessel for the next few decades sounded like a solid plan. Not to be outdone, the U.S. Coast Guard admitted in March that it needed to "reassess baseline metrics" for its Polar Security Cutter program, which is just a fancy way of saying they're nowhere close to figuring it out. These decisions are set to haunt U.S. operations in Antarctica way past 2050, ensuring a legacy of strategic blunders.

The result of these independent yet equally baffling decisions is a significant reduction in the U.S. physical presence in Antarctica. This not only spells trouble for American scientists but also signals a retreat in U.S. geopolitical influence in the region. With Russia flexing its icebreaker superiority and China rapidly catching up, the U.S. seems to have forgotten the basics: regular funding for Antarctic research, a strategy that doesn't belong in a museum labeled "A Masterclass in Budgetary Woes and Strategic Apathy"



## EUROPOL CYBERCRIME TRAINING COMPETENCY FRAMEWORK 2024

What the world really needs is another deep dive into the "Europol Cybercrime Training Competency Framework 2024". Here, the brilliant minds at Europol decided to state the obvious: cybercrime is bad, and we need to stop it. They've created this framework to outline the skills necessary to combat cybercrime, because apparently, it's not enough to just be good with a computer anymore. Who knew?

Moving on to the "Approach and Scope." It's where they tell us that the framework isn't exhaustive. So, in other words, they spent all this time putting together a document that doesn't cover everything. Fantastic. They also mention that it's not an

endorsement of a specific unit structure, which is code for "please don't blame us if this doesn't work out."

The "Roles" section is where things get spicy. They've listed various roles like "Heads of cybercrime units" and "Cybercrime analysts," each with their own set of required skills. Because, as we all know, the key to stopping cybercriminals is making sure everyone has the right title.

And finally, the "Skill Sets" section. This is where they list all the skills you'll need to fight cybercrime, from digital forensics to cybercrime legislation. It's a bit like reading a job description that asks for a candidate who speaks 12 languages, can code in 15 different programming languages, and has climbed Mount Everest—twice.

The document tells us we need to be prepared to tackle cybercrime with a specific set of skills, roles, and a dash of optimism. Because, in the fight against cybercrime, it's not just about having the right tools; it's about having a document that says you have the right tools.



## HUMANOID ROBOT

Another riveting document that promises to revolutionize the world as we know it—this time with humanoid robots that are not just robots, but super-duper, AI-enhanced, almost-human robots, because, of course, what could possibly go wrong with replacing humans with robots in hazardous jobs? It's not like we've seen this movie plot a dozen times.

First off, let's talk about the technological marvels these robots are equipped with—end-to-end AI and multi-modal AI algorithms. These aren't your grandma's robots that just weld car doors; these robots can make decisions! Because when we think of what we want in a robot, it's the ability to make complex decisions, like whether to screw in a bolt or take over the world.

And let's not forget the economic implications. A forecasted increase in the Total Addressable Market (TAM) and a delightful reduction in the Bill of Materials (BOM) cost, in layman's terms, they're going to be cheaper and everywhere. Great news for all you aspiring robot overlords out there!

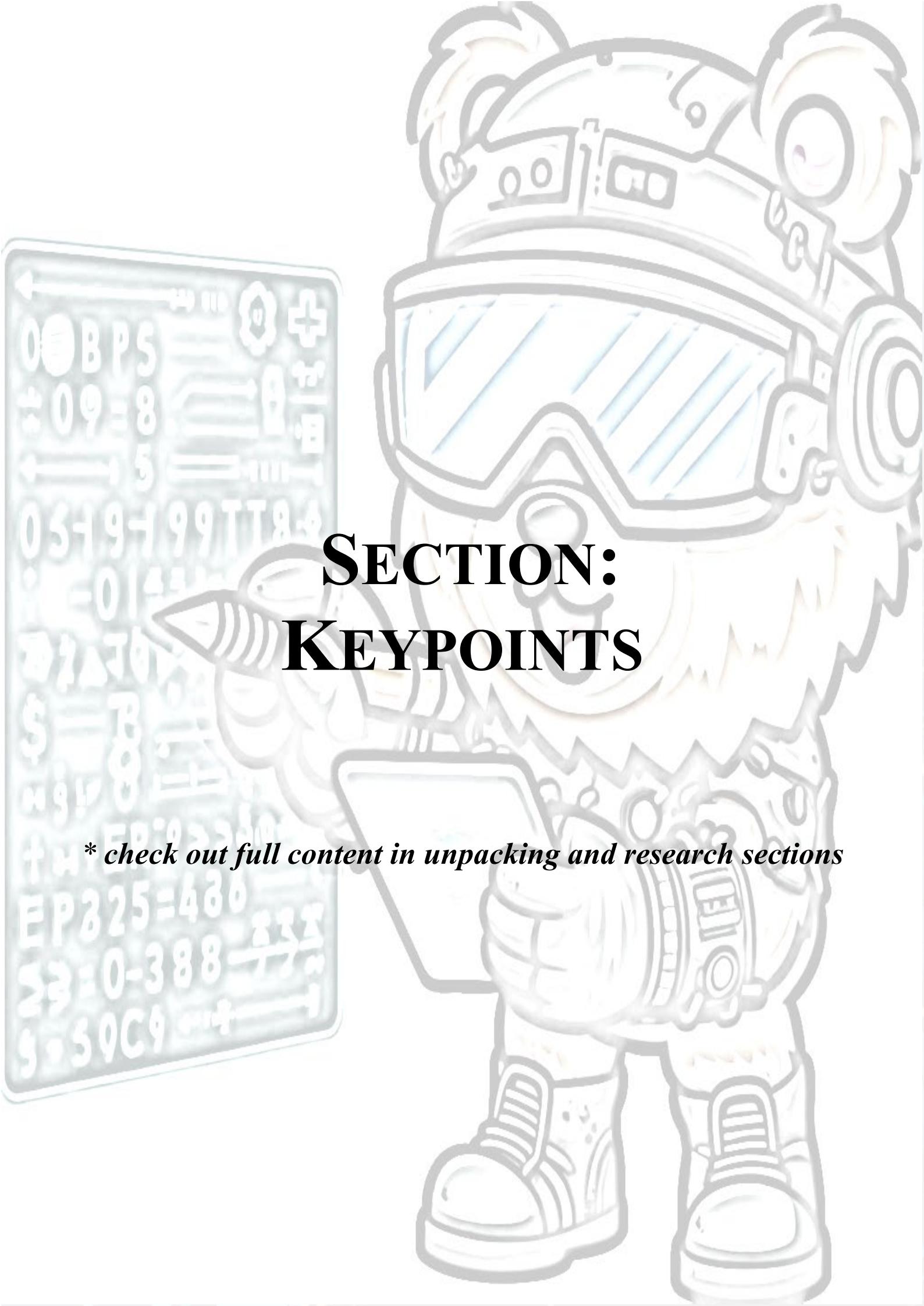
Now, onto the labor market implications. These robots are set to replace humans in all those pesky hazardous and repetitive tasks. Because why improve workplace safety when you can just send in the robots? It's a win-win: robots don't sue for negligence, and they definitely don't need healthcare—unless you count the occasional oil change and software update.

In conclusion, if you're a security professional or an industry specialist, this document is not just a read; it's a glimpse into a future where robots could potentially replace your job. So, embrace the innovation, but maybe keep your human security guard on speed dial, just in case the robots decide they're not too thrilled with their job description. After all, who needs humans when you have robots that can read reports and roll their eyes sarcastically at the same time?

Read more: [Boosty](#) | [Sponsr](#) | [TG](#)



STARRY SECURITY



# SECTION: KEYPOINTS

\* *check out full content in unpacking and research sections*

#### A. Maritime Security



The paper titled "Quantifying the econometric loss of a cyber-physical attack on a seaport" presents a comprehensive study on the economic impacts of cyber-physical attacks on maritime infrastructure which are critical components of global trade and supply chains and a significant contribution to understanding the vulnerabilities and potential economic repercussions of cyber-physical threats in the maritime sector.

Maritime cyber-security is an increasingly important area of concern for the maritime industry, as emerging technologies such as the Internet of Things (IoT), digital twins, 5G, and Artificial Intelligence (AI) are becoming more prevalent in the sector. The convergence and digitization of Information Technology (IT) and Operational Technology (OT) have driven the transformation of digital supply routes and maritime operations, expanding cyber-threat surfaces.

##### 1) Key Points

- Increased marine traffic and larger ships with more capacity have led to challenges in maneuvering in existing channels and seaports, lowering safety margins during cyber-incidents. Today's ships are also more heavily instrumented, increasing the threat surface for cyber-attacks.
- The US Coast Guard reported a 68% increase in marine cyber-incidents, and recent studies show that cyber risks within marine and maritime technology are present and growing as new solutions are adopted.
- While digitization in shipping offers productivity gains, physical safety, lower carbon footprints, higher efficiency, lower costs, and flexibility, there are vulnerabilities in large CPS sensor networks and communication systems.
- A survey of mariners found that 64% of respondents believed that a port had already experienced significant physical damage caused by a cyber security incident, and 56% thought a merchant vessel had already

experienced significant physical damage caused by a cyber security incident.

##### 2) Secondary Points

- **Emerging Technologies:** The maritime sector is adopting new technologies across offices, ships, seaports, offshore structures, and more. These technologies include the Internet of Things (IoT), digital twins, 5G, and Artificial Intelligence (AI).
- **Supply Chain Digitization:** Supply chains are also using more Information Technology (IT), introducing digital vulnerabilities. The convergence of IT and Operational Technology (OT) is transforming digital supply routes and maritime operations, expanding cyber-threat surfaces.
- **Cyber Threats:** Nation-state actors and organized crime have the resources and motivation to trigger a cyber-attack on Critical National Infrastructure (CNI), such as large-scale Cyber-Physical Systems, which include maritime operations.
- **Cyber-Physical Systems:** The integration of physical processes with software and communication networks, known as Cyber-Physical Systems, is a significant part of the maritime sector's digital transformation. However, it also introduces new cybersecurity challenges.
- **Impact of Cyber-Attacks:** Cyber-attacks on maritime infrastructure can have significant economic impacts, affecting not only the targeted seaport but also the broader global maritime ecosystem and supply chains.

##### 3) Realistic modelling

- The case study is based on a European seaport in Spain and a class of container ship that routinely docks at the same port. Both port and ship are modeled from real-world data, from their physical attributes to their digital attributes.
- The Port of Valencia generates nearly 51% of Spain's Gross Domestic Product (GDP) and is a significant player in European and global supply chains that connect Asia and the Americas. Any disruption to this port would result in a direct economic loss to Spain and ripple through different physical nodes and value chains.
- Existing literature on Supply Chain Risk Management (SCRM) provides numerous frameworks and models for types and sources of risks as well as mitigation strategies. However, little is known about supply chain cyber-risks in an Industry 4.0 technology landscape.
- The Econometric Model (EM) by using a fully quantitative model with comprehensive nodal network mapping to accurately represent the end-to-end life cycle of a product and calculate the econometric impact of an existing supply chain network.
- Disruptions within a Cyber-Physical System (CPS), like maritime transportation, can propagate between the physical layers and the cyber layer due to high interconnections and interdependency. Risk factors range from physical to cyber and also static to dynamic.

- The approach uses a more dynamic cyber-physical approach to risk to present quantified results to the public and measure the change in their understanding of cyber-risk regarding global supply chains.

#### 4) Framework

The framework uses a "hybrid" modeling method that takes partially mapped supply chains and uses predictive analytics to infill the missing parts. This approach avoids the underestimation of risk by capturing hidden vulnerabilities and correlations stemming from the unseen or unknown parts of a given supply chain. The supply chain risk model is the first of its kind, as it is a quantitative model that incorporates global trade patterns and supply networks, product flow mapping, and correlation across different product groups and industries.

The combined CyPEM stages give public and private organizations the ability to stress test their supply chain resiliency by estimating the cost and time to recover after different cyber-attack scenarios. The framework includes quantitative risk models that emulate major components of global supply chains and their uncertainties to estimate time delays and economic losses resulting from contingent business interruption (CBI). Downtime is measured on the order of days or hours caused by cyber-physical disruptions to a given supply chain node.

The framework has been designed to provide some dynamic automation when calculating cyber-physical econometric losses. Some of the cyber-attack scenario variables can be altered "live" during various stages to explore a range of econometric outcomes. The framework is designed to provide analytics for different supply chain arcs or sectors and can be used to communicate quantifiable cyber-physical risk to a wide audience.

- Define Industry, intermediate parts, and final products:** This stage involves identifying the industry, intermediate parts, and final products that are relevant to the supply chain being analyzed.
- Define Network where nodes are suppliers and edges are product/part flows:** In this stage, the supply chain network is defined, with nodes representing suppliers and edges representing product or part flows.
- Calculate Disruption using cyber-physical risk assessment and a port throughput model:** This stage involves calculating the disruption caused by a cyber-physical attack using a risk assessment model and a port throughput model.
- Propagate Disruption in the wider network:** In this stage, the disruption is propagated through the wider supply chain network to assess the impact on other nodes and edges.
- Calculate the industry loss and loss distributions:** The final stage involves calculating the industry loss and loss distributions resulting from the disruption.

#### B. Offensive companies II



The Equation Group is classified as an advanced persistent threat (APT) and is known for its sophisticated cyber-espionage activities. It has been active since at least 2001 and is renowned for its complex and highly advanced malware tools and techniques. The group has been involved in numerous cyber operations targeting a wide range of sectors and countries, including government, military, telecommunications, aerospace, energy, nuclear research, and financial institutions.

The Equation Group is suspected of being tied to the NSA's Tailored Access Operations (TAO) unit. This connection is suggested by several factors:

- I) Similarities Between the Equation Group and the NSA*
- Sophistication and Resources:** The Equation Group is recognized for its highly sophisticated cyber capabilities, including the development and use of complex malware and zero-day exploits. The group's operations, which span decades and target a wide range of sectors globally, indicate a level of resources and expertise consistent with a state-sponsored entity like the NSA.
- Similarities to NSA Tools and Techniques:** Analysis of the Equation Group's malware and exploits reveals significant similarities to those known to be used by the NSA. For instance, the use of specific encryption algorithms (RC5, RC6, RC4, AES) and obfuscation techniques mirrors those documented in NSA operations. Additionally, the malware's operational hours and the targeting of specific countries align with U.S. interests, suggesting a connection to the NSA.
- Shadow Brokers Leak:** In 2016, a group known as the Shadow Brokers leaked a trove of cyber tools and exploits they claimed to have stolen from the Equation Group. Analysis of these tools showed they exploited vulnerabilities in software and hardware in ways that

were highly sophisticated and previously unknown, suggesting the involvement of an entity with extensive cyber warfare capabilities, like the NSA.

- **Snowden Documents:** Documents leaked by Edward Snowden have provided indirect evidence linking the Equation Group to the NSA. Certain codenames and operational details found in the Snowden documents match those associated with the Equation Group's activities, reinforcing the belief that the group operates under the NSA's auspices.
- **Shared Zero-Day Exploits:** Research has shown that the Equation Group had access to zero-day exploits before they were used in other known NSA-associated malware, such as Stuxnet and Flame. This temporal precedence suggests that the Equation Group either is part of the NSA or works closely with it, sharing tools and exploits for cyber operations.
- **Expert Analysis and Attribution:** Cybersecurity experts and researchers, including those from Kaspersky Lab, have pointed to the technical sophistication, targeting patterns, and operational security of the Equation Group as being indicative of a state-sponsored actor with objectives aligning with those of the NSA. While direct attribution is challenging in cyberspace, the accumulated evidence and expert consensus lean strongly towards the Equation Group being part of, or affiliated with, the NSA.

## 2) The TAC Discussion on EQGRP

Vault 7 from WikiLeaks provides a rare glimpse into the internal reactions and operational challenges faced by national intelligence agencies following the exposure of their cyber capabilities, emphasizing the ongoing need for security enhancements and strategic adjustments in cyber operations.

- **Collaborative Efforts and Shared Capabilities:** EQGRP was not a single entity but a collective term used to describe a range of cyber capabilities primarily managed by the NSA's TAO and the CIA's IOC. This highlights the collaborative nature of cyber operations between these two key U.S. intelligence entities.
- **Joint Development and Authorship:** The discussion indicates that some parts of the cyber implants associated with EQGRP were co-authored by both the CIA and the NSA. This joint authorship underlines the integrated approach to developing cyber tools and strategies.
- **Differences in Operational Processes:** There were notable differences in the processes or the lack thereof for re-using cyber capabilities between the CIA IOC and NSA TAO. These differences could potentially impact the efficiency and security of cyber operations.
- **Lessons Learned:** The leak and subsequent public exposure of these activities have led to significant introspection within these agencies. The discussion reflects a keen interest in learning from the incident to prevent future compromises and enhance the security of cyber operations.

- **Importance of High-Quality Threat Intelligence:** The discussion also underscores the value of high-quality threat intelligence, as demonstrated by Kaspersky's report, which played a crucial role in uncovering these activities. The agencies recognize the need to understand and mitigate the implications of such intelligence findings on national security.

### 3) Thoughts

- **Collaborative Nature of U.S. Cyber Operations:** it emphasizes that U.S. cyber operations are not the domain of any single agency. Instead, they involve collaboration across various intelligence agencies, including the NSA and the CIA. This collaborative approach is typical of complex cyber operations which require a range of skills and resources that no single agency could effectively manage alone.
- **Role of CIA's IOC:** The CIA's Information Operations Center (IOC) is highlighted as a significant player in the activities attributed to the Equation Group. The IOC's involvement suggests that the operations of the Equation Group are more broadly based within the U.S. intelligence community than previously thought.
- **Misattribution and Misunderstandings:** the challenges and potential inaccuracies involved in attributing cyber activities to specific groups or agencies. Due to the clandestine nature of intelligence efforts and the intricate technicalities of cyber warfare, pinpointing responsibility accurately is exceedingly difficult. Consequently, there is a tendency to oversimplify matters by attributing all advanced cyber operations to the NSA
- **Public Perception and Media Simplification:** The criticism of media and public discourse often centers on their tendency to oversimplify the narrative surrounding cyber operations by exclusively attributing them to the NSA. This oversimplification fails to acknowledge the complex reality of inter-agency collaboration and the distributed nature of cyber intelligence and warfare capabilities.
- **Importance of a Broader View:** It necessitates a more sophisticated comprehension of how the U.S. government conducts cyber operations. Acknowledging the involvement of various agencies beyond the NSA is essential for a thorough grasp of U.S. capabilities and strategies in cyberspace.

### C. Choosing Secure and Verifiable Technologies



The document "Choosing Secure and Verifiable Technologies" provides comprehensive guidance for organizations on procuring digital products and services with a focus on security from the design phase through the lifecycle of the technology. It emphasizes the critical importance of selecting technologies that are inherently secure to protect user privacy and data against the increasing number of cyber threats. It outlines the responsibility of customers to evaluate the security, suitability, and associated risks of digital products and services. It advocates for a shift towards products and services that are secure-by-design and secure-by-default, highlighting the benefits of an approach, including enhanced resilience, reduced risks, and lower costs related to patching and incident response.

#### 1) Audience

- **Organizations that procure and leverage digital products and services:** This encompasses a wide range of entities known as procuring organizations, purchasers, consumers, and customers. These organizations are the main focus of the guidance provided in the document, aiming to enhance their decision-making process in procuring digital technologies.
- **Manufacturers of digital products and services:** The document also addresses the manufacturers of digital technologies, providing them with insights into security-by-design considerations. This is intended to guide manufacturers in developing technologies that meet the security expectations of their customers.
- **Organization Executives and Senior Managers:** Leaders who play a crucial role in decision-making and strategy formulation for their organizations.
- **Cyber Security Personnel and Security Policy Personnel:** Individuals responsible for ensuring the

security of digital technologies within their organizations.

- **Product Development Teams:** Those involved in the creation and development of digital products and services, ensuring these offerings are secure by design.
- **Risk Advisers and Procurement Specialists:** Professionals who advise on risk management and specialize in the procurement process, ensuring that digital technologies procured do not pose undue risks to the organization.

#### 2) Shifting the Balance of Cybersecurity Risk

The document "Choosing Secure and Verifiable Technologies" relates to another whitepaper "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default", led by the Cybersecurity and Infrastructure Security Agency (CISA), is a collaborative effort aimed at guiding technology manufacturers in enhancing the security of their products. This publication is significant as it represents an international endeavor to mitigate exploitable vulnerabilities in technology utilized by both government and private sector organizations. The whitepaper is supported by a coalition of global security agencies, including CISA, FBI, NSA, and international partners from Australia, Canada, New Zealand, the United Kingdom, Germany, and the Netherlands.

#### 3) External procurement considerations

External procurement considerations are divided into the pre-purchase and post-purchase phases to ensure secure and informed decisions when acquiring digital products and services. The pre-purchase phase focuses on several key areas to ensure that organizations make informed and secure choices when procuring digital products and services. The post-purchase phase addresses several critical aspects of managing digital products and services after acquisition. These aspects are crucial for ensuring ongoing security, compliance, and operational efficiency.

#### 4) Internal Procurement Considerations

Internal procurement considerations are divided into three phases: pre-purchase, purchasing, and post-purchase. Each phase addresses specific aspects that organizations need to consider internally when procuring digital products and services. The pre-purchase phase focuses on ensuring that the internal aspects of an organization align with the procurement of digital products and services. This phase involves consultations and evaluations across various departments within the organization to ascertain that the product or service being considered meets the organizational needs and security standards. The purchasing phase involves critical evaluations and decisions that ensure the alignment of the procurement process with organizational goals and security requirements. The post-purchase phase involves ensuring that the procured digital products and services continue to align with the organization's security, operational, and strategic goals. This phase requires ongoing assessments and management practices to address any emerging risks or changes in the organization's or product's environment.

#### D. Europol Cybercrime Training Competency Framework 2024



The Europol Cybercrime Training Competency Framework 2024 encompasses a wide range of documents related to cybercrime training, competency frameworks, strategies, and legislation. These materials (as compilation by Europol) collectively aim to enhance the capabilities of law enforcement, judiciary, and other stakeholders in combating cybercrime effectively.

- **Purpose of the Framework:** The framework aims to identify the required skill sets for key actors involved in combating cybercrime.
- **Development Process:** The framework was developed following a multi-stakeholder consultation process. This included contributions from various European bodies such as CEPOL, ECTEG, Eurojust, EJCN, and EUCTF.
- **Strategic Context:** The renewed framework is part of the European Commission's action plan aimed at enhancing the capacity and capabilities of law enforcement authorities in digital investigations.
- **Functional Competences:** The framework identifies the essential functional competences required by law enforcement authorities to effectively combat cybercrime. It emphasizes the specific skills needed for cybercrime investigations and handling digital evidence, rather than general law enforcement skills.
- **Strategic Capacity Building:** The framework is intended as a tool for strategic capacity building within law enforcement and judicial institutions. It aims to enhance the competencies that are crucial for the effective handling of cybercrime cases.
- **Role Descriptions:** Detailed descriptions of the main functions and skill sets for various roles are provided throughout the framework. These roles include heads of

cybercrime units, team leaders, general criminal investigators, cybercrime analysts, and specialized experts among others. Each role is tailored to address specific aspects of cybercrime and digital evidence handling.

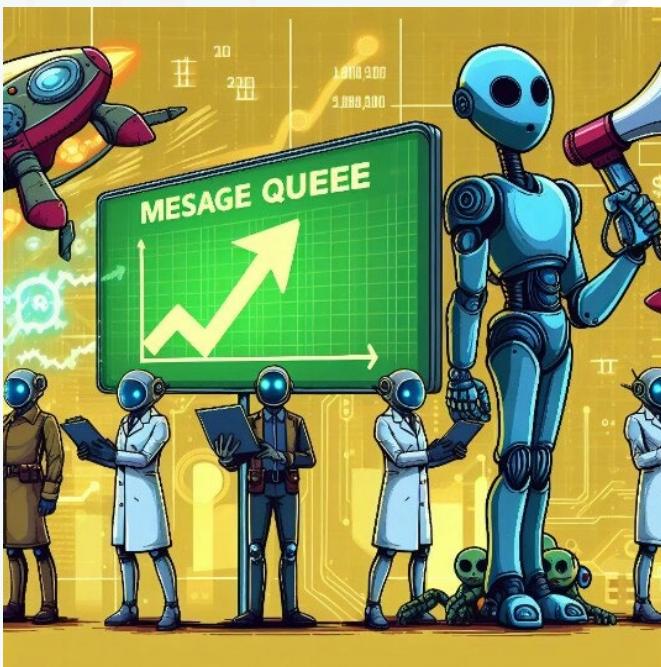
- **Skill Sets and Levels:** The framework outlines specific skill sets required for each role and the desired levels of proficiency. These skill sets include digital forensics, network investigation, programming, and cybercrime legislation, among others. The framework emphasizes the importance of having tailored skills that are directly applicable to the challenges of cybercrime.

##### 1) Roles

- **Heads of Cybercrime Units:** These individuals are responsible for overseeing cybercrime units, making informed decisions about cybercrime cases, coordinating resources, and prioritizing policing activities. They need to have a comprehensive understanding of the unit's capabilities and provide necessary training and tools for staff. Effective communication and relationship management skills, especially in English, are essential for interacting with international stakeholders.
- **Team Leaders:** Team leaders manage cybercrime investigations within their specific areas. They supervise ongoing investigations, coordinate with senior management, and ensure their team is equipped with the necessary training and tools. Like heads of units, they require practical experience in evaluating operational activities and strong communication skills.
- **General Criminal Investigators:** These investigators increasingly encounter cyber elements in various crimes. They need a fundamental understanding of the digital world, including how to handle electronic evidence at crime scenes and utilize open-source intelligence (OSINT) effectively.
- **Cybercrime Analysts:** Analysts are involved in collecting and analyzing data to produce actionable intelligence and strategic insights. They need to process large amounts of data from diverse sources and translate these into concise reports. Sharing information with wider audiences and participating in strategic meetings are also part of their role.
- **Cybercrime Investigators:** These are specialized investigators with a deeper understanding of data extraction and online information acquisition. They lead cybercrime investigations and are involved in training other trainers within the law enforcement community.
- **Specialized Cybercrime Experts:** These experts have specialized knowledge in specific areas of cybercrime, such as OSINT, Dark Web, cryptocurrencies, and IoT devices. They provide operational support in investigations and need to keep their skills updated through peer exchanges at national and international levels.

- **Digital Forensic Examiners (Investigators):** These professionals focus on identifying, recovering, and analyzing digital evidence. They are familiar with various operating systems, forensic tools, and have skills in scripting and programming. They prepare evidence for advanced decryption tasks and report their findings.
  - **Cyber-attack Response Experts:** These experts handle the technical response to cyber-attacks, cooperating with various stakeholders like Computer Emergency Response Teams (CERTs) and IT departments. They are responsible for preserving digital evidence and ensuring its integrity for judicial processes.
  - **First Responders:** First responders are usually the initial law enforcement officers at the scene of a cyber incident. They need basic knowledge of digital forensics and cybercrime, and their responsibilities include identifying and securing electronic evidence according to national regulations and best practices.
  - **Trial and Appeal Judges:** Judges dealing with cybercrime cases need to integrate cyber evidence effectively into the judicial process. They should acquire and maintain updated knowledge of cybercrime and electronic evidence.
  - **Prosecutors and Investigative Judges:** These legal professionals direct criminal investigations involving cyber elements, assess the collection of electronic evidence, and present cases in court. They require a basic understanding of the digital world and the ability to use intelligence from various sources, including OSINT, to complement their investigations
- 2) Skills
- **Digital Forensics:** Involves identification, preservation, acquisition, validation, analysis, interpretation, documentation, and presentation of electronic evidence from digital sources. Key areas include live data forensics, OS forensics, file system forensics, mobile forensics, network forensics, IoT forensics, cloud forensics, and cryptography.
  - **Network Investigation and Administration:** Pertains to understanding network functions, conducting investigative activities within networks, and analyzing traffic data to identify indicators of compromise. Skills include network administration, live network data acquisition, network forensic and traffic data analysis, and expertise in cyber-crime investigations and evidence retention.
  - **Programming and Scripting:** Utilized for building information systems and automating tasks to support investigations and data analysis. Important programming languages include Python, JavaScript, Java, and C++, among others. Skills also cover backend, frontend development, and full-stack development.
  - **Reporting and Presenting Cybercrime Investigative Data:** Encompasses documentation, note-taking, and final report writing across various report types. It emphasizes the importance of structured reporting that is factual, credible, and admissible in court. Presentation skills include synthesizing information and adapting complex technical topics for non-technical audiences.
  - **Analysis and Visualization:** Involves applying data analysis techniques to describe, illustrate, and summarize cybercrime data to find patterns, trends, and actionable knowledge plus data gathering, research design, statistical methods, visualization best practices, and ethical considerations in handling crime data.
  - **Cybercrime Legislation:** Relates to understanding legislation governing cyber-criminal activity, including national legislation on cybercrime and electronic evidence, privacy laws, GDPR, EU regulations on data retention, and international court rulings.
  - **General Cybercrime Knowledge:** Covers information related to cyber-enabled and cyber-dependent crime, cybercrime trends, threats, and modi operandi, as well as an understanding of cybersecurity.
  - **Specific Cybercrime Knowledge:** Refers to unique skills obtained through specialized training in specific areas of cybercrime. Areas include OSINT, Dark Web, blockchains and cryptocurrencies, intrusion analysis and incident response, ethical hacking, threat intelligence, and malware analysis and reverse engineering.
  - **Crime Scene Management & Electronic Evidence Handling:** Pertains to standards and best practices in identifying and seizing electronic evidence at crime scenes. Skills include collecting, packaging, transferring, and storing devices that may contain electronic evidence, as well as conducting on-the-scene interviews and supporting victims.
  - **Cybercrime Investigative Techniques:** Consists of skills required for a cybercrime investigation, such as intelligence gathering techniques, processing and interpreting data, tracing suspects online and offline, online undercover work, cybercriminal interrogation/questioning, and investigation risk management

*E. Market Insights. Simple Solutions Are Just Too Cheap, Spending More is Always Better*



Message brokers are essential components in modern distributed systems, enabling seamless communication between applications, services, and devices. They act as intermediaries that validate, store, route, and deliver messages, ensuring reliable and efficient data exchange across diverse platforms and programming languages. This functionality is crucial for maintaining the decoupling of processes and services, which enhances system scalability, performance, and fault tolerance.

Major players in this market include Kinesis, Cisco IoT, Solace, RabbitMQ, Apache Kafka, ApacheMQ, IBM MQ, Microsoft Azure Service Bus, and Google Cloud IoT, each offering unique capabilities and serving a wide range of industries from financial services to healthcare and smart cities.

- Market Share:** The percentage each broker holds in the queueing, messaging, and processing category.
- Number of Users:** The total number of companies or devices using the broker.
- Corporate Users:** The number of enterprise customers using the broker.
- Revenue Distribution:** The distribution of companies using the broker based on their revenue.
- Geographical Coverage:** The percentage of users based in different regions.

#### Broker's market share and user base

Broker	Market Share	Number of Users	Corporate Users
RabbitMQ	28.24%	15,851	14,651
Apache Kafka	39.73%	22,244	22,244
Apache ActiveMQ	5.79%	9,604	9,604
IBM MQ	7.12%	4,060	4,060
Microsoft Azure Service Bus	3.84%	12,870	4,609

EMQX	N/A	20,000+	500+
HiveMQ	N/A	20,000+	500+
PubNub	N/A	330M devices	500+
ThingsBoard	N/A	Thousands	500+
AWS IoT	N/A	718	718
Azure IoT	14.90%	1,396	1,396
Google Cloud IoT	18.65%	1,790	1,790
Cisco IoT	9.52%	129	129
Solace	5.33%	133	133
Amazon Kinesis	1.20%	216	216

#### Broker's revenue and geo coverage

Broker	Customer	Revenue Distribution	Geographical Coverage (%)
RabbitMQ	Currys, Beckman Coulter	< \$50M: 39%, \$50M-\$1B: 16%, > \$1B: 40%	US: 46.15%, India: 9.72%, UK: 9.70%
Apache Kafka	LinkedIn, Uber, Netflix	< \$50M: 52%, \$50M-\$1B: 18%, > \$1B: 24%	US: 51.91%, India: 12.95%, UK: 8.28%
Apache ActiveMQ	Infosys, Fujitsu, Panasonic	< \$50M: 24%, \$50M-\$1B: 43%, > \$1B: 33%	US: 47%, UK: 6%, India: 6%
IBM MQ	American Airlines, Aflac	< \$50M: 39%, \$50M-\$1B: 16%, > \$1B: 40%	US: 59.39%, UK: 8.70%, India: 8.67%
Microsoft Azure Service Bus	Infosys, Fujitsu, Panasonic	< \$50M: 40%, \$50M-\$1B: 17%, > \$1B: 39%	US: 48.02%, UK: 14.97%, India: 8.98%
EMQX	IoT sector companies	N/A	50+ countries
HiveMQ	Fortune 500 companies	N/A	US: 60%
PubNub	US companies	N/A	Global
ThingsBoard	IoT sector companies	N/A	50+ countries
AWS IoT	Global companies	N/A	US: 52.12%, India: 13.26%, UK: 8.84%
Azure IoT	Global companies	N/A	US: 47.72%, India: 14.04%, UK: 8.73%
Google Cloud IoT	Global companies	N/A	US: 48.77%, India: 16.58%, Germany: 6.39%
Cisco IoT	Infosys, Cisco Systems, Wipro, AT&T, Cognizant	< \$50M: 25%, \$50M-\$1B: 17%, > \$1B: 47%	US: 50%, India: 9%
Solace	Large enterprises in finance, telecom, manufacturing	< \$50M: 16%, \$50M-\$1B: 29%, > \$1B: 49%	US: 38.18% France: 10.91% Canada: 10%
Amazon Kinesis	Siemens, Microsoft, Oracle, Cisco	< \$50M: 25%, \$50M-\$1B: 15%, > \$1B: 60%	US: 61.78% India: 10.47% UK: 8.38%

#### F. Cybersecurity & Antarctica



In April, the U.S. National Science Foundation (NSF) announced that it would not support any new field research this season due to delays in upgrading the McMurdo Station. The NSF and the U.S. Coast Guard also announced cuts that will jeopardize the U.S.'s scientific and geopolitical interests in the region for decades to come. Specifically, in April, the NSF announced that it would not renew the lease of one of its two Antarctic research vessels, the Laurence M. Gould. Prior to this, in October 2023, the NSF announced that it would operate only one research vessel in the coming decades.

Additionally, in March, the U.S. Coast Guard announced that it needed to "reassess baseline metrics" for its long-delayed Polar Security Cutter program, a vital program for U.S. national interests at both poles. Decisions made today will have serious consequences for U.S. activities in Antarctica well beyond 2050.

The State Department has refrained from announcing U.S. foreign policy interests in the Antarctic region, and the White House appears satisfied with an outdated and inconsistent national strategy for Antarctica from the last century. The U.S. Congress has also not responded to scientists' calls.

As a result, on April 1, the NSF's Office of Polar Programs announced that it is putting new fieldwork proposals on hold for the next two seasons and will not be soliciting new fieldwork proposals in Antarctica.

Ships capable of operating in polar seas are becoming increasingly in demand and difficult to build. Facing significant challenges in the ice-class ship and vessel project, the U.S. Coast Guard announced in March that it would "shift baseline timelines" for developing new icebreaker projects.

The outcome of these seemingly independent decisions will be a reduction in the U.S. physical presence in Antarctica. This will have negative consequences not only for American scientists but also for U.S. geopolitics in the region, especially

considering Russia's total superiority in icebreaker vessels and China's catching up.

The U.S. has missed the most important aspects: adequate and regular funding for Antarctic scientific research, a new national strategy for Antarctica (the current strategy was published in June 1994), and lawmakers' understanding of the importance of U.S. interests and decisions in Antarctica. The inability to fund the operational and logistical support necessary for U.S. scientific research and geopolitical influence effectively means the dominance of Russia and China in the Antarctic region, as no other country, including traditional Antarctic stakeholders like Chile, Australia, and Sweden, can surpass the existing and growing scientific potential of Russia and China.

##### *1) Economic consequences*

###### *a) Disruption of Scientific Research and Operations*

- **Impact on Research Missions:** Cyberattacks can disrupt the operations of research vessels and stations, leading to delays or cancellations of scientific missions. This can result in the loss of valuable research data and increased costs associated with rescheduling and extending missions.
- **Operational Delays:** Disruptions to navigation systems, communication networks, and other critical operational technologies can lead to significant delays in maritime operations. This can increase operational costs and reduce the efficiency of research and supply missions.

###### *b) Increased Operational Costs*

- **Mitigation and Recovery Costs:** The costs associated with mitigating and recovering from cyberattacks can be substantial. This includes expenses related to incident response, system restoration, and implementing additional cybersecurity measures to prevent future attacks.
- **Insurance Premiums:** Cyberattacks can lead to higher insurance premiums for maritime companies operating in Antarctica. Insurers may increase premiums to cover the heightened risk of cyber incidents, adding to the overall operational costs.

###### *c) Supply Chain Disruptions*

- **Impact on Logistics:** Cyberattacks can disrupt the supply chain by affecting the transportation of goods and essential supplies to and from Antarctica. This can lead to shortages of critical supplies, increased transportation costs, and delays in the delivery of goods.
- **Economic Ripple Effects:** Disruptions in the supply chain can have ripple effects on the broader economy, affecting industries that rely on timely deliveries of goods and materials. This can lead to increased costs and reduced productivity across multiple sectors.

###### *d) Loss of Sensitive Data and Intellectual Property*

- **Data Breaches:** Cyberattacks can result in the theft of sensitive data, including research findings, proprietary information, and personal data of crew members and researchers. The loss of such data can have significant

economic implications, including the loss of competitive advantage and potential legal liabilities.

- **Intellectual Property Theft:** The theft of intellectual property, such as proprietary research data and technological innovations, can undermine the economic value of scientific research and development efforts in Antarctica.

*e) Impact on National Security and Geopolitical Interests*

- **Geopolitical Tensions:** Cyberattacks on maritime operations in Antarctica can exacerbate geopolitical tensions, particularly if they are attributed to nation-state actors. This can lead to increased defense and security expenditures as countries seek to protect their interests in the region.
- **Strategic Vulnerabilities:** The disruption of maritime operations can expose strategic vulnerabilities, potentially affecting national security and economic stability. This can lead to increased investments in cybersecurity and defense measures, diverting resources from other critical areas.

*2) Non-economic consequences*

The non-economic consequences of cyberattacks on the maritime industry in Antarctica are significant and multifaceted. They include threats to safety and human life, environmental damage, geopolitical tensions, disruption of scientific research, and operational challenges.

*a) Safety and Human Life*

- **Crew Safety:** Cyberattacks can compromise the safety of crew members by disrupting critical systems such as navigation, communication, and engine controls. This can lead to accidents, groundings, or collisions, putting lives at risk.
- **Search and Rescue Operations:** Disruptions to communication and navigation systems can hinder search and rescue operations, making it difficult to locate and assist vessels in distress. This can result in delayed response times and increased risk to human life.

*b) Environmental Impact*

- **Pollution and Spills:** Cyberattacks that disrupt navigation or engine control systems can lead to accidents that result in oil spills or the release of hazardous materials into the fragile Antarctic

environment. Such incidents can have long-lasting detrimental effects on marine ecosystems and wildlife.

- **Ecosystem Damage:** The Antarctic region is home to unique and sensitive ecosystems. Cyber-induced accidents can cause significant damage to these ecosystems, affecting biodiversity and the overall health of the environment.

*c) Geopolitical and Security Implications*

- **Geopolitical Tensions:** Cyberattacks on maritime operations in Antarctica can exacerbate geopolitical tensions, particularly if they are attributed to nation-state actors. This can lead to increased military presence and heightened security measures in the region, potentially escalating conflicts.
- **National Security:** The disruption of maritime operations can expose strategic vulnerabilities, affecting national security. This is particularly relevant for countries with significant interests in Antarctica, as cyberattacks can undermine their ability to protect and assert their claims and interests in the region.

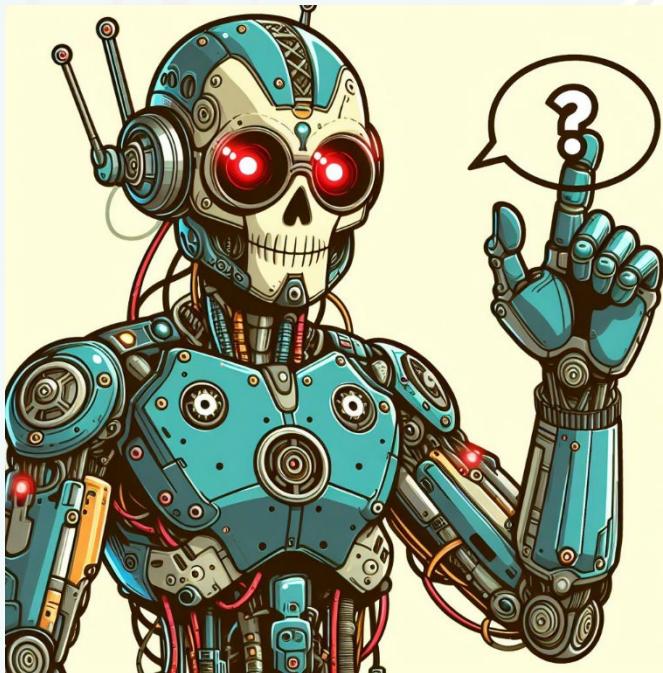
*d) Disruption of Scientific Research*

- **Impact on Research Missions:** Cyberattacks can disrupt the operations of research vessels and stations, leading to delays or cancellations of scientific missions. This can result in the loss of valuable research data and hinder scientific progress in understanding climate change, marine biology, and other critical areas.
- **Data Integrity:** Cyberattacks can compromise the integrity of scientific data, leading to inaccurate or incomplete research findings. This can undermine the credibility of scientific research and affect policy decisions based on such data.

*e) Operational and Logistical Challenges*

- **Operational Disruptions:** Cyberattacks can disrupt the day-to-day operations of maritime vessels, affecting everything from navigation to cargo handling. This can lead to significant logistical challenges, including delays in the delivery of essential supplies and equipment to research stations.
- **Communication Breakdown:** Disruptions to communication systems can isolate vessels and research stations, making it difficult to coordinate activities and respond to emergencies. This can increase the risk of accidents and hinder effective crisis management.

## G. Humanoid Robot



Humanoid robots are advanced machines designed to mimic human form and behavior, equipped with articulated limbs, advanced sensors, and often the ability to interact socially. These robots are increasingly being utilized across various sectors, including healthcare, education, industry, and services, due to their adaptability to human environments and their ability to perform tasks that require human-like dexterity and interaction.

In healthcare, humanoid robots assist with clinical tasks, provide emotional support, and aid in-patient rehabilitation. In education, they serve as interactive companions and personal tutors, enhancing learning experiences and promoting social integration for children with special needs. The industrial sector benefits from humanoid robots through automation of repetitive and hazardous tasks, improving efficiency and safety. Additionally, in service industries, these robots handle customer assistance, guide visitors, and perform maintenance tasks, showcasing their versatility and potential to transform various aspects of daily life.

### 1) Market Forecasts for Humanoid Robots

The humanoid robot market is poised for substantial growth, with projections indicating a multi-billion-dollar market by 2035. Key drivers include advancements in AI, cost reductions, and increasing demand for automation in hazardous and manufacturing roles.

- **Goldman Sachs Report (January 2024):**
  - **Total Addressable Market (TAM):** The TAM for humanoid robots is expected to reach \$38 billion by 2035, up from an initial forecast of \$6 billion. This increase is driven by a fourfold rise in shipment estimates to 1.4 million units.
  - **Shipment Estimates:** The base case scenario predicts a 53% compound annual growth rate (CAGR) from 2025 to 2035, with shipments

reaching 1.4 million units by 2035. The bull case scenario anticipates shipments hitting 1 million units by 2031, four years ahead of previous expectations.

- **Cost Reductions:** The Bill of Materials (BOM) cost for high-spec robots has decreased by 40% to \$150,000 per unit in 2023, down from \$250,000 the previous year, due to cheaper components and a broader domestic supply chain.

- **Data Bridge Market Research:** The global humanoid robot market is expected to grow from \$2.46 billion in 2023 to \$55.80 billion by 2031, with a CAGR of 48.5% during the forecast period.
- **SkyQuestt:** The market is projected to grow from \$1.48 billion in 2019 to \$34.96 billion by 2031, with a CAGR of 42.1%.
- **GlobeNewswire:** The global market for humanoid robots, valued at approximately \$1.3 billion in 2022, is anticipated to expand to \$6.3 billion by 2030, with a CAGR of 22.3%.
- **The Business Research Company:** The market is expected to grow from \$2.44 billion in 2023 to \$3.7 billion in 2024, with a CAGR of 51.6%. By 2028, the market is projected to reach \$19.69 billion, with a CAGR of 51.9%.
- **Grand View Research:** Market Size: The global humanoid robot market was estimated at \$1.11 billion in 2022 and is expected to grow at a CAGR of 21.1% from 2023 to 2030.
- **Goldman Sachs (February 2024):** In a blue-sky scenario, the market could reach up to \$154 billion by 2035, comparable to the global electric vehicle market and one-third of the global smartphone market as of 2021.
- **Macquarie Research:** Under a neutral assumption, the global humanoid robot market is expected to reach \$107.1 billion by 2035, with a CAGR of 71% from 2025 to 2035.

### 2) Key Drivers and Trends

- **Technological Advancements:** Significant progress in AI, particularly in end-to-end AI and multi-modal AI algorithms, is accelerating product iterations and improving robot capabilities.
- **Cost Reductions:** The availability of cheaper components and improvements in design and manufacturing techniques are driving down costs, making humanoid robots more economically viable.
- **Labor Market Implications:** The demand for robots to handle hazardous and dangerous jobs is elevated by national policies, with potential applications in manufacturing, disaster rescue, and elderly care.
- **Investment and Market Dynamics:** Increased investments from supply chains, startups, and listed companies, particularly in the US and Asia, are driving market growth. Government support, especially from China, is also a significant factor.

### 3) Increased Investments and Funding

The sources highlight the significant investments and funding pouring into the humanoid robotics sector, driven by the potential of this emerging technology and the involvement of major tech companies and investors.

- Figure AI, a startup developing humanoid robots, raised a staggering \$675 million in a Series B funding round, valuing the company at \$2.6 billion post-money. The funding round attracted prominent investors, including Jeff Bezos (through Bezos Expeditions), Microsoft, Nvidia, OpenAI Startup Fund, Amazon Industrial Innovation Fund, Intel Capital, Align Ventures, and ARK Invest.
- OpenAI, the company behind ChatGPT, entered into a collaboration agreement with Figure AI to develop next-generation AI models for humanoid robots, combining OpenAI's research with Figure's robotics expertise.
- Microsoft is investing \$95 million in Figure AI and will provide its Azure cloud services for AI infrastructure, training, and storage.
- Nvidia, a leading chipmaker, is investing \$50 million in Figure AI.
- Amazon's investment arm, the Intel Capital venture fund are also participating in the funding round.
- Norwegian startup 1X Technologies raised \$100 million in funding from OpenAI.
- Agility Robotics, backed by Amazon in 2022, is testing its humanoid robots in Amazon warehouses.
- Sanctuary AI is developing a humanoid robot called Phoenix.
- Increased Interest from Venture Capital Firms: Venture capital firms like Parkway Venture Capital, Align Ventures, ARK Venture Fund, Aliya Capital Partners, and Tamarack are investing in humanoid robotics startups. The funding landscape remains challenging, but the AI boom has given hope to startups in the humanoid robotics space.
- The potential government support, especially from China, is a significant factor driving market growth

### 4) Industry insights

Humanoid robots offer significant potential benefits for military applications, including enhanced capabilities, operational efficiency, and cost savings. However, their deployment also raises ethical, legal, and technical challenges that must be carefully managed.

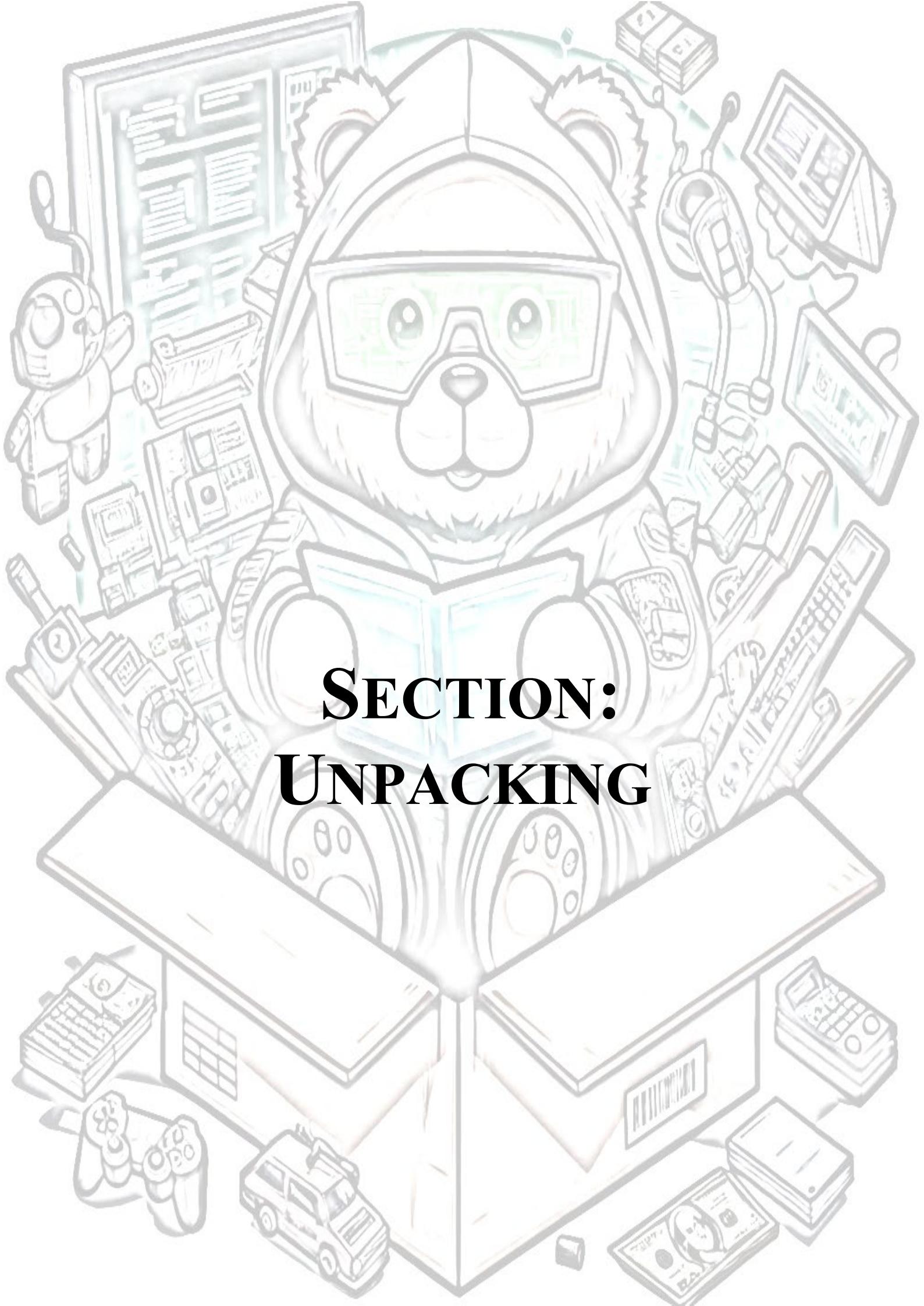
- **Manufacturing:** Humanoid robots are used in manufacturing for tasks such as assembly, quality control, and material handling.
- **Healthcare:** In healthcare, humanoid robots assist with patient care, rehabilitation, and surgery.

- **E-commerce and Warehousing:** Humanoid robots are employed in e-commerce and warehousing to handle logistics, such as sorting and transporting goods.
- **Customer Service and Hospitality:** Humanoid robots are used in customer service roles, such as concierges, receptionists, and guides.
- **Security:** Humanoid robots are used in security to patrol areas, detect intrusions, and monitor for safety hazards.
- **Education and Research:** In educational settings, humanoid robots are used as teaching aids and research tools.
- **Entertainment:** Humanoid robots are also used in entertainment, such as performing at events, acting as tour guides in museums, and even conducting orchestras.
- **Military:** Humanoid robots could be used in military applications for tasks such as reconnaissance, bomb disposal, and logistics support.
- **Cyberbiosecurity:** Humanoid robots could play a role in cyberbiosecurity by monitoring and protecting biological data and systems from cyber threats.
- **Oil and Gas Industry:** In the oil and gas industry, humanoid robots could be used for inspection, maintenance, and repair of offshore platforms and pipelines.
- **Mining:** Humanoid robots could be used in mining to perform tasks such as drilling, ore extraction, and safety inspections.
- **Financial Services and Stock Markets:** Humanoid robots could assist in financial services by providing customer support, conducting transactions, and analyzing market data.
- **Real Estate Development:** In real estate, humanoid robots could be used for property inspections, maintenance, and customer interactions.
- **Food and Grocery Industry:** Humanoid robots could be used in the food and grocery industry for tasks such as stocking shelves, preparing food, and delivering groceries.
- **Aircraft:** In the aircraft industry, humanoid robots could assist with maintenance, inspections, and assembly of aircraft components.
- **Maritime and Shipping:** Humanoid robots could be used in maritime and shipping for tasks such as cargo handling, ship maintenance, and safety inspections.
- **Smart Cities:** In smart cities, humanoid robots could be used for various tasks such as traffic management, public safety, and maintenance of infrastructure.

Read more: [Boosty](#) | [Sponsr](#) | [TG](#)



STARRY SECURITY



# **SECTION: UNPACKING**



# MARITIME SECURITY



**Abstract** – This document presents a comprehensive analysis of the multifaceted impacts of cyber-physical attacks on seaport operations, with a focus on quantifying econometric losses. The analysis will delve into various aspects, including the direct economic losses incurred, the ripple effects on different industry sectors, the specific vulnerabilities and consequences of cyber-physical attacks, and the security measures within maritime ports. This analysis is particularly beneficial for security professionals, IT experts, policymakers, and stakeholders across various industries, offering insights into the magnitude of potential disruptions and guiding the development of robust cyber resilience strategies. The insights gained from this analysis are crucial for enhancing the preparedness and response to cyber threats in critical national infrastructure, thereby safeguarding economic stability and national security.

#### A. Introduction

The paper titled "Quantifying the econometric loss of a cyber-physical attack on a seaport" presents a comprehensive study on the economic impacts of cyber-physical attacks on maritime infrastructure which are critical components of global trade and supply chains and a significant contribution to understanding the vulnerabilities and potential economic repercussions of cyber-physical threats in the maritime sector.

The core of the research revolves around the development and application of an econometric (EC) model designed to quantify the economic losses resulting from cyber-physical attacks on seaports. This model, referred to as the Cyber Physical Econometric Model (CyPEM), is a five-part framework that integrates various aspects of cyber-physical systems, economic impact analysis, and risk management strategies. The methodology involves a systematic approach to model the initial economic impacts of a cyber-physical attack, which, although starting locally, can have far-reaching global effects due to the interconnected nature of global trade and supply chains.

The results highlight the significant economic vulnerabilities of seaports to cyber-physical attacks. Through the application of the CyPEM, the researchers were able to quantify the potential econometric losses, demonstrating that the economic impact of such attacks can be profound, affecting not only the targeted

seaport but also the broader global maritime ecosystem and supply chains. The model's findings underscore the cascading effects of disruptions in seaport operations, which can lead to substantial economic losses both locally and globally. It serves as a concrete example of how the model can be used to estimate the economic fallout of cyber-physical attacks on seaports.

It also highlights the convergence of IT and Operational Technology as a transformative force in the maritime sector, creating digital supply routes and modernizing maritime operations. However, this convergence also enlarges the cyber-threat surface, making critical maritime infrastructure more susceptible to cyber-attacks. The threat is not only from common cybercriminals but also from nation-state actors and organized crime groups that possess the resources and motivation to target Critical National Infrastructure (CNI), such as large-scale Cyber-Physical Systems, which include vital maritime operations.

#### B. Benefits of the proposed solution:

- Quantifies the potential economic impact of a cyber-physical attack on a seaport, both locally and globally
- Helps to identify potential vulnerabilities and weaknesses in the supply chain, allowing for better preparation and response to cyber-attacks
- Can be adapted to analyze different cyber-physical systems

#### C. Drawbacks of the proposed solution:

- Small sample size of the survey used to gauge public perception of cyber-physical risk in maritime transport
- May require specialized knowledge to use effectively
- Complexity of the model may make it difficult for some stakeholders to understand and utilize the results
- Does not consider other potential consequences of cyber-physical attacks, such as environmental or safety impacts.

#### D. Application

The proposed framework is useful for quantifying econometric losses resulting from a cyber-physical event. The econometric outputs of a cyber-physical attack on the port allowed for a comparison of the actual risk for cyber-security to the public's perceived risk concerning maritime cyber-threats and how it affects them.

Moving forward, the tool can be used by stakeholders to better quantify and understand their specific cyber-physical risks, including insurance-related corporations with regional and/or global exposure to contingent business interruption losses and organizations whose industrial activity is exposed to global supply chains. The ability to exchange individual framework steps also allows for the modeling of other sectors besides marine and maritime scenarios and the consideration of cyber-physical interruptions at different nodes.

Governmental organizations, port authorities, freight transport and logistic actors, and trade associations may also be interested in the proposed framework, as it can help policymakers gain a greater understanding of their risk landscape and identify particular weaknesses or dependencies that, if exploited, could have a significant impact on the national

economy. Compliance with international governance frameworks, such as the European Union's National Intelligence Service (NIS) Directive, also requires the identification of essential services providers.

The main limitation of the survey was the number of participants, and future work could push the survey to a wider audience and employ cyclic networks when modeling supply chains. Different cyber-physical risk assessments or throughput simulations could also be used to calculate the EM of other sectors or locations. As a cyber-attack can attack the same system in divergent geographic “nodes,” modeling and assessing the EM loss could provide novel results.

#### *E. Maritime cyber-security*

Maritime cyber-security is an increasingly important area of concern for the maritime industry, as emerging technologies such as the Internet of Things (IoT), digital twins, 5G, and Artificial Intelligence (AI) are becoming more prevalent in the sector. The convergence and digitization of Information Technology (IT) and Operational Technology (OT) have driven the transformation of digital supply routes and maritime operations, expanding cyber-threat surfaces.

The integration of digital technologies into critical operations in the maritime sector introduces significant cyber-physical vulnerabilities that could lead to larger global disruptions. As the maritime sector accelerates into digitization, it is critical to understand and quantify the potential impacts of cyber-physical disruptions.

##### *1) Key Points*

- Increased marine traffic and larger ships with more capacity have led to challenges in maneuvering in existing channels and seaports, lowering safety margins during cyber-incidents. Today's ships are also more heavily instrumented, increasing the threat surface for cyber-attacks.
- The US Coast Guard reported a 68% increase in marine cyber-incidents, and recent studies show that cyber risks within marine and maritime technology are present and growing as new solutions are adopted.
- While digitization in shipping offers productivity gains, physical safety, lower carbon footprints, higher efficiency, lower costs, and flexibility, there are vulnerabilities in large CPS sensor networks and communication systems.
- A survey of mariners found that 64% of respondents believed that a port had already experienced significant physical damage caused by a cyber security incident, and 56% thought a merchant vessel had already experienced significant physical damage caused by a cyber security incident.

##### *2) Secondary Points*

- **Emerging Technologies:** The maritime sector is adopting new technologies across offices, ships, seaports, offshore structures, and more. These technologies include the Internet of Things (IoT), digital twins, 5G, and Artificial Intelligence (AI).
- **Supply Chain Digitization:** Supply chains are also using more Information Technology (IT), introducing

digital vulnerabilities. The convergence of IT and Operational Technology (OT) is transforming digital supply routes and maritime operations, expanding cyber-threat surfaces.

- **Cyber Threats:** Nation-state actors and organized crime have the resources and motivation to trigger a cyber-attack on Critical National Infrastructure (CNI), such as large-scale Cyber-Physical Systems, which include maritime operations.
- **Cyber-Physical Systems:** The integration of physical processes with software and communication networks, known as Cyber-Physical Systems, is a significant part of the maritime sector's digital transformation. However, it also introduces new cybersecurity challenges.
- **Impact of Cyber-Attacks:** Cyber-attacks on maritime infrastructure can have significant economic impacts, affecting not only the targeted seaport but also the broader global maritime ecosystem and supply chains.

#### *F. Cyber-physical threat*

The maritime sector is increasingly vulnerable to cybersecurity threats, which can have far-reaching consequences for other areas due to the interconnected nature of modern transportation. As technology continues to advance, the likelihood of disruptive events caused by malicious cyber-attacks is growing, as evidenced by recent reports and academic research. To understand the potential scale of these disruptions, it is important to examine the impact of major supply chain disruptions on the target of the attack and the rest of the associated supply chain. These events resulted in many business interruption insurance claims, with the majority of claims coming from areas outside of the directly affected regions.

Current cyber defense capabilities are unlikely to prevent all cyber-physical catastrophes, making it crucial to quantify and understand the effects of such events. It focuses on the interdependencies in today's global supply chains and presents an econometric model (EM) that allows organizations to transition from a qualitative assessment to a more robust quantitative treatment of supply chain risk.

The world's manufacturing supply networks are susceptible to disruption by cyber-attacks, which can propagate through the network and physically and economically affect adjacent, preceding, and succeeding nodes with negative impacts. Cyber-attacks using IT/OT networks and computing systems can cause short-term losses, Denial of Service (DoS), long-term equipment damage, loss of customer trust, delays in shipment, and loss of strategic advantages due to leaks and compromised sensitive information. Digital cyber-attacks can also have real physical consequences, such as unfulfilled demands in supply transportation and manufacturing.

##### *1) Key points*

- With the increasing rate of technological growth, there is a growing likelihood of disruptive events triggered by malicious cyber-attacks in the maritime sector.
- Economic and insured losses stemming from supply chain disruptions are among the top emerging risks for global corporations and insurers.

- As current cyber defense capabilities are unlikely to prevent all cyber-physical catastrophes, it is crucial to quantify and understand the effect of such events.
- The research focuses on how major supply chain disruptions affect the target of the attack and the rest of the associated supply chain, presented in a classical graph format of "nodes" representing assets and "edges" connecting nodes.
- The econometric model (EM) allows organizations to transition from a qualitative assessment to a more robust quantitative treatment of supply chain risk.
- Integrating the EM with MaCRA's dynamic cyber-physical risk model, the combined model allows a user to derive quantitative modeled losses to improve understanding of the global supply chain's cyber-physical risks, leading to increased cyber-resilience and system trustworthiness.

## 2) *Realistic modelling*

- The case study is based on a European seaport in Spain and a class of container ship that routinely docks at the same port. Both port and ship are modeled from real-world data, from their physical attributes to their digital attributes.
- The Port of Valencia generates nearly 51% of Spain's Gross Domestic Product (GDP) and is a significant player in European and global supply chains that connect Asia and the Americas. Any disruption to this port would result in a direct economic loss to Spain and ripple through different physical nodes and value chains.
- Existing literature on Supply Chain Risk Management (SCRM) provides numerous frameworks and models for types and sources of risks as well as mitigation strategies. However, little is known about supply chain cyber-risks in an Industry 4.0 technology landscape.
- The Econometric Model (EM) by using a fully quantitative model with comprehensive nodal network mapping to accurately represent the end-to-end life cycle of a product and calculate the econometric impact of an existing supply chain network.
- Disruptions within a Cyber-Physical System (CPS), like maritime transportation, can propagate between the physical layers and the cyber layer due to high interconnections and interdependency. Risk factors range from physical to cyber and also static to dynamic.
- The approach uses a more dynamic cyber-physical approach to risk to present quantified results to the public and measure the change in their understanding of cyber-risk regarding global supply chains.

## G. Framework

The framework uses a "hybrid" modeling method that takes partially mapped supply chains and uses predictive analytics to infill the missing parts. This approach avoids the underestimation of risk by capturing hidden vulnerabilities and correlations stemming from the unseen or unknown parts of a given supply chain. The supply chain risk model is the first of its kind, as it is a quantitative model that incorporates global

trade patterns and supply networks, product flow mapping, and correlation across different product groups and industries.

The combined CyPEM stages give public and private organizations the ability to stress test their supply chain resiliency by estimating the cost and time to recover after different cyber-attack scenarios. The framework includes quantitative risk models that emulate major components of global supply chains and their uncertainties to estimate time delays and economic losses resulting from contingent business interruption (CBI). Downtime is measured on the order of days or hours caused by cyber-physical disruptions to a given supply chain node.

The framework has been designed to provide some dynamic automation when calculating cyber-physical econometric losses. Some of the cyber-attack scenario variables can be altered "live" during various stages to explore a range of econometric outcomes. The Port of Valencia cyber-physical attack scenario is used to compute a range of econometric losses, based on the severity of the attack and the duration of the delay (i.e., 3, 5, and 7 days). This tool allows users to proactively manage supply chain risks by anticipating interdependencies and correlations in supply chains and the effects of cyber-triggered disruptive events before they can occur. The quantified results are also critical for measuring gaps in perceived vs. actual risk as understood by experts and laypeople.

The framework is designed to provide analytics for different supply chain arcs or sectors and can be used to communicate quantifiable cyber-physical risk to a wide audience.

- **Define Industry, intermediate parts, and final products:** This stage involves identifying the industry, intermediate parts, and final products that are relevant to the supply chain being analyzed.
- **Define Network where nodes are suppliers and edges are product/part flows:** In this stage, the supply chain network is defined, with nodes representing suppliers and edges representing product or part flows.
- **Calculate Disruption using cyber-physical risk assessment and a port throughput model:** This stage involves calculating the disruption caused by a cyber-physical attack using a risk assessment model and a port throughput model.
- **Propagate Disruption in the wider network:** In this stage, the disruption is propagated through the wider supply chain network to assess the impact on other nodes and edges.
- **Calculate the industry loss and loss distributions:** The final stage involves calculating the industry loss and loss distributions resulting from the disruption.

The first two stages of the framework involve creating acyclic network graphs using United Nations Commodity Trade Statistics and EM product flows to establish product dependencies. Once the product dependencies are established, trade data from the UN Commodity Trade Statistics is incorporated to create a network that includes storage and transportation nodes, as well as the supply chain flow of components based on inter- and intra-industry dependencies.

The next stage of the framework is network definition, which looks beyond product dependencies to consider a country's

manufacturing and transportation to determine product flows and arcs. While the model currently uses an acyclic network to represent the flow of products without creating feedback loops, future modeling at this stage can be exchanged for another type of network depending on the end use of the entire framework. Data used to define and create future networks could include the period of data, the flow (i.e., import/export), commodity codes, trade values, net weights, quantity, and statistics from the reporter (i.e., Port of Valencia).

The proposed network is a hybrid one, which merges the product dependency graph (or tree) from stage one and relevant trade data from stage two. This step ensures that the econometric model can account for movements of trade across country and sector boundaries within product categories. The resulting hybrid network is key to determining the econometric losses from a cyber-physical disruption in the later stages of the CyPEM framework. However, one limitation of this method is that the hybrid network is pre-defined, which could mean fundamental changes to the underlying trade models in the longer-term.

Predictive analytics can improve the product dependency graphs in the earlier stages of the framework, which subsequent stages rely on for accuracy and depth of detail. CyPEM collects data from numerous sources and legacy systems to provide a complete view of the supply chain, and subsequent analyses are conducted to uncover useful information and achieve boosted intelligence. Prescriptive analytics are used to automate complex decisions and proactively and dynamically update recommendations based on changing events to take advantage of these predictions and provide added value to the project classification tools. Using these networks to pre-define many of the market and dependency attributes, and how they affect the rest of the network, while keeping the actual disruption events (and all their individual pieces) more dynamic.

The CyPEM framework involves calculating disruptions using two models: a maritime cyber-risk assessment model and a cyber-physical model of the Port of Valencia's throughput. The maritime cyber-risk assessment model takes a cyber-physical attack chain to show a range of potential risks and outcomes, depending on the success of each segment of an attack chain. The attack chain used in this model has been verified with actual data and testbed experiments, which have been cross-referenced with legitimate system vulnerabilities on ships known to enter

the Port of Valencia and with the port authorities from Tam et al. (2022) and Tam et al. (2021).

The second part of calculating disruptions is to take the cyber-physical risks and their outcomes, and to predict the overall disruption effect to the Port of Valencia. To do this, a cyber-physical model of the Port of Valencia's throughput was developed. This process is very similar to stages one and two but built for the internal workings of a single port instead of an entire global network. The proposed method allows the model to be more highly detailed, even modeling the individual ships and terminal cranes (including their type) to accurately determine port downtimes in terms of hours and also in percentages.

In order for the throughput model to simulate port operations for the Port of Valencia, certain parameters that describe traffic and flow within the port must be considered. This includes information characterizing the following: (i) arrival process, (ii) average quantity of containers per port call (in Twenty-foot Equivalent Units, or TEUs), (iii) service time distribution per vessel, (iv) proportion of containers destined to be transshipped, and (v) the mean container dwell time. The analysis can be simulated multiple times to output a range of realistic downtime values that correspond to different attack chains and cyber-physical attack outcomes.

The cyber-attack triggered disruption is observed to decrease the production/transportation capability of nodes and have a ripple effect to successor nodes. Again, in an acyclic network, effects progress downstream in a one-way direction. However, if circular supply chains are integrated into the framework as a future next step, disruption patterns and results could be very different. In this instance of CyPEM, cyber-triggered disruptions are propagated through the network in a similar manner to other types of disruptions (e.g., Levalle and Nof, 2017). A global cyber-attack can differ from other natural disaster disruptions, which can be localized geographically, while cyber-attacks tend to occur where the targeted systems are located. Therefore, a single digital threat, such as WannaCry and NotPetya (Branquinho, 2018), could trigger cyber incidences in multiple geographic regions or reach across several sectors (e.g., health, manufacturing) if similar underlying technology is used.



# OFFENSIVE COMPANIES

## II



**Abstract – This document provides a analysis of publicly known private companies involved in nation-state offensive cyber operations. The analysis delves into various aspects of the inventory, including the nature of the companies listed, the types of capabilities they offer, and the geopolitical implications of their services.**

**The extract provided is of high quality, aggregating publicly available information without disclosing sensitive or confidential data. It serves as a valuable resource for security professionals, offering insights into the landscape of private sector participation in offensive cyber operations.**

#### A. What is the Equation Group?

The Equation Group is classified as an advanced persistent threat (APT) and is known for its sophisticated cyber-espionage activities. It has been active since at least 2001 and is renowned for its complex and highly advanced malware tools and techniques. The group has been involved in numerous cyber operations targeting a wide range of sectors and countries, including government, military, telecommunications, aerospace, energy, nuclear research, and financial institutions

#### B. Equation Technologies

##### 1) Cyber capabilities

- **Remote Access Tools and Malware Platforms:** The Equation Group employs multiple remote access tools and has developed several malware platforms of high complexity and sophistication, such as EquationDrug, DoubleFantasy, Equestre (same as EquationDrug), TripleFantasy, GrayFish, Fanny, and EquationLaser. These tools are designed for espionage and have self-destruct mechanisms to reduce forensic evidence.
- **Firmware Reprogramming:** One of the most advanced techniques used by the Equation Group is the ability to reprogram hard drive firmware. This capability allows the group to persist on infected systems undetectably and effectively makes their operations invisible and indestructible.

- **Encryption and Obfuscation:** The Equation Group frequently uses sophisticated encryption schemes, including the RC5, RC6, RC4, AES cryptographic functions, and various hashes, to protect its malware and communications. This level of encryption and the strategies employed to camouflage its activity are indicative of the group's advanced capabilities.
- **Exploitation of Zero-Day Vulnerabilities:** The group has access to and has used zero-day exploits, which are vulnerabilities unknown to the software vendors and the public at the time of exploitation. For example, the Equation Group used two zero-day exploits in Fanny before they were integrated into Stuxnet, indicating access to these vulnerabilities before other known cyber-attack groups.
- **USB-Based Reconnaissance Tools:** To map air-gapped networks, which are not connected to the Internet, the Equation Group developed USB stick-based reconnaissance malware. This capability is significant for penetrating secure military facilities, intelligence organizations, and nuclear facilities.
- **Exploit Frameworks and Post-Exploitation Tools:** The Equation Group uses a variety of exploit frameworks and post-exploitation tools, such as DanderSpritz, which is a full-featured framework used after exploiting a machine. DanderSpritz contains a wide variety of modules for persistence, reconnaissance, lateral movement, and bypassing antivirus engines.
- **Firewall Exploit Chain:** The Equation Group has developed a near-complete exploit kit targeting major firewall manufacturers. This kit includes exploits like EXTRABACON (CVE-2016-6366) for gaining access to Cisco ASA and PIX firewalls, and EPICBANANA (CVE-2016-6367) for planting command and control shellcode.
- **Interdiction Techniques:** The group has used interdiction techniques, such as intercepting physical goods and replacing them with Trojanized versions, to deliver malware. This method demonstrates the group's capability to infect targets not only through the web but also in the physical world.
- 2) **Equation Group's Malware**
  - **EquationDrug:** A complex malware platform that provides the group with a full-featured espionage platform.
  - **DoubleFantasy:** A validator-style malware used to confirm the target is of interest and then deploy further malware.
  - **Fanny:** A worm that uses two zero-day exploits to map air-gapped networks via USB sticks.
  - **GrayFish:** A platform that resides entirely in the registry, encrypting its payload and storing it in a virtual file system.

One of the most powerful tools in their arsenal is a module known only by a cryptic name: “nls\_933w.dll”, which allows them to reprogram the hard drive firmware of over a dozen different hard drive brands. This capability is an astonishing technical accomplishment and is testament to the group’s abilities.

### 3) Remote Access Tools

The Equation Group employs multiple remote access tools (RATs) and is known for using zero-day exploits. These tools are capable of overwriting disk drive firmware, further demonstrating the group's advanced capabilities:

- **UnitedRake (UR):** A remote access tool that can target Windows machines. It is an extensible and modular framework provided with many plugins that perform different information collection functions.
- **DoubleFeature:** A post-exploitation tool that logs the use of other malware tools on the infected machine, providing a unique source of knowledge pertaining to Equation Group tools.
- **EquationLaser, EquationDrug, DoubleFantasy, Equestre (same as EquationDrug), TripleFantasy, GrayFish, Fanny, and EquationLaser:** Custom attack platforms, trojans, worms, and backdoors used by the Equation Group.

The Equation Group's use of these tools and exploits does not change the path of a normal kill chain, making them a formidable opponent. Their operations are characterized by professionalism, organization, and a focus on retaining stealth

### C. Relationship Between the Equation Group and the NSA

The Equation Group is suspected of being tied to the NSA's Tailored Access Operations (TAO) unit. This connection is suggested by several factors:

#### 1) Similarities Between the Equation Group and the NSA

- **Sophistication and Resources:** The Equation Group is recognized for its highly sophisticated cyber capabilities, including the development and use of complex malware and zero-day exploits. The group's operations, which span decades and target a wide range of sectors globally, indicate a level of resources and expertise consistent with a state-sponsored entity like the NSA.
- **Similarities to NSA Tools and Techniques:** Analysis of the Equation Group's malware and exploits reveals significant similarities to those known to be used by the NSA. For instance, the use of specific encryption algorithms (RC5, RC6, RC4, AES) and obfuscation techniques mirrors those documented in NSA operations. Additionally, the malware's operational hours and the targeting of specific countries align with U.S. interests, further suggesting a connection to the NSA.
- **Shadow Brokers Leak:** In 2016, a group known as the Shadow Brokers leaked a trove of cyber tools and exploits they claimed to have stolen from the Equation Group. Analysis of these tools showed they exploited

vulnerabilities in software and hardware in ways that were highly sophisticated and previously unknown, suggesting the involvement of an entity with extensive cyber warfare capabilities, like the NSA.

- **Snowden Documents:** Documents leaked by Edward Snowden have provided indirect evidence linking the Equation Group to the NSA. Certain codenames and operational details found in the Snowden documents match those associated with the Equation Group's activities, reinforcing the belief that the group operates under the NSA's auspices.
- **Shared Zero-Day Exploits:** Research has shown that the Equation Group had access to zero-day exploits before they were used in other known NSA-associated malware, such as Stuxnet and Flame. This temporal precedence suggests that the Equation Group either is part of the NSA or works closely with it, sharing tools and exploits for cyber operations.
- **Expert Analysis and Attribution:** Cybersecurity experts and researchers, including those from Kaspersky Lab, have pointed to the technical sophistication, targeting patterns, and operational security of the Equation Group as being indicative of a state-sponsored actor with objectives aligning with those of the NSA. While direct attribution is challenging in cyberspace, the accumulated evidence and expert consensus lean strongly towards the Equation Group being part of, or affiliated with, the NSA.

#### 2) Differences Between the Equation Group and the NSA

While the Equation Group is primarily focused on cyber espionage and the creation and deployment of advanced malware, the NSA has a broader mission that includes both intelligence gathering and national security operations. The NSA's activities encompass a wide range of operations including signal intelligence, cyber-security, and global monitoring, with the aim of collecting and analyzing data that pertains to national security.

The NSA operates globally and is involved in various types of intelligence activities, which include but are not limited to cyber operations. It is structured to support broader U.S. intelligence and defense operations, whereas the Equation Group is specifically focused on sophisticated cyber espionage.

#### 3) Mission of the Equation Group vs. NSA's Mission

The mission of the Equation Group revolves around conducting cyber espionage to gather intelligence, often by deploying malware that can infiltrate and persist in target systems undetected. Their operations are characterized using zero-day exploits, sophisticated malware, and techniques designed to breach high-value targets and remain hidden.

In contrast, the NSA's mission is more comprehensive and includes the collection and processing of global signals intelligence to inform U.S. national defense and foreign policy decisions. The NSA's activities are not limited to cyber operations; they also include a wide array of signal intelligence and information assurance products and services designed to

protect U.S. information systems and produce foreign signals intelligence information

#### 4) Central Intelligence Agency's Information Operations Center (IOC)

The Central Intelligence Agency's Information Operations Center (IOC) plays a crucial role in the agency's expanded mission, which now includes covert paramilitary operations alongside its traditional intelligence-gathering activities. The IOC, one of the CIA's largest divisions, has shifted its focus from counterterrorism to offensive cyber operations, reflecting the evolving nature of global threats and the increasing importance of cyber warfare in national security.

The IOC's foundation as the agency's digital and cyber operations hub was further solidified with the establishment of the Directorate for Digital Innovation (DDI) in 2015. This new directorate, the first new directorate in fifty years, was created to modernize the CIA's IT systems and further operationalize its cyber capabilities. It brought together the spy agency's CIO shop, cyber capabilities, and open-source intelligence efforts under one roof, aiming to provide CIA analysts with better IT tools for traditional espionage work and to locate and understand the "digital dust" left behind by actors in the cyber domain.

The creation of the DDI and the emphasis on the IOC's role in cyber operations underscore the CIA's recognition of the digital domain as a critical battlefield. The agency's efforts to integrate digital and cyber capabilities into its operations reflect a broader trend within the U.S. intelligence community to adapt to the challenges posed by the digital age, including cyber threats, electronic surveillance, and information warfare

#### 5) CIA's Engineering Development Group (EDG)

The CIA Engineering Development Group (EDG) is tasked with the development, testing, and operational support of all backdoors, exploits, and malicious payloads used by the CIA in cyber operations. This group plays a critical role in creating the tools and techniques necessary for conducting cyber espionage and cyber warfare.

EDG's responsibilities include ensuring that the CIA maintains a cutting-edge capability in penetrating adversary systems and networks, leveraging vulnerabilities in software and hardware to gather intelligence or achieve other operational objectives.

#### 6) Technical Aspects of CIA Cyber Operations (TAC)

The CIA's cyber operations involve sophisticated tools and techniques for intelligence gathering from adversary systems and networks. This includes the use of advanced tradecraft in cyber espionage, which is supported by the technical expertise within the agency.

Cyber Security Officers within the CIA are responsible for protecting agency data and systems against threats. They utilize sophisticated tools and knowledge of CIA Information Technology (IT) to monitor, evaluate, and manage IT risk. This includes identifying current threats, mitigating vulnerabilities, and anticipating future challenges.

The Operations Support Branch (OSB) of the CIA, part of its cyber-intelligence division, specializes in physical access operations, indicating a technical capability to develop tools for

cyberintelligence missions on short notice. This highlights the technical agility and innovation within the CIA's cyber operations

#### 7) The TAC Discussion on EQGRP

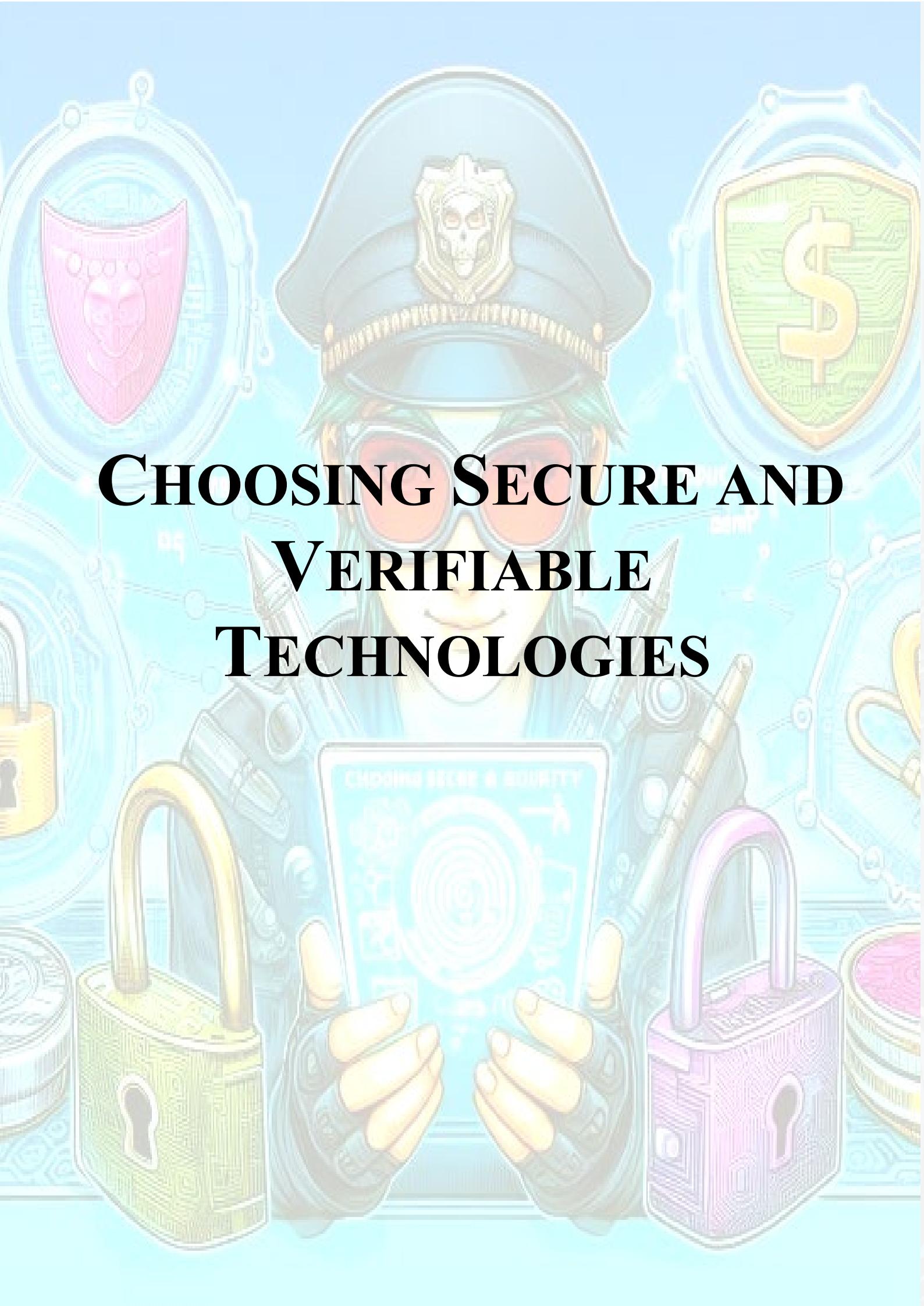
Vault 7 from WikiLeaks provides a rare glimpse into the internal reactions and operational challenges faced by national intelligence agencies following the exposure of their cyber capabilities, emphasizing the ongoing need for security enhancements and strategic adjustments in cyber operations.

- **Collaborative Efforts and Shared Capabilities:** EQGRP was not a single entity but a collective term used to describe a range of cyber capabilities primarily managed by the NSA's TAO and the CIA's IOC. This highlights the collaborative nature of cyber operations between these two key U.S. intelligence entities.
- **Joint Development and Authorship:** The discussion indicates that some parts of the cyber implants associated with EQGRP were co-authored by both the CIA and the NSA. This joint authorship underlines the integrated approach to developing cyber tools and strategies.
- **Differences in Operational Processes:** There were notable differences in the processes or the lack thereof for re-using cyber capabilities between the CIA IOC and NSA TAO. These differences could potentially impact the efficiency and security of cyber operations.
- **Lessons Learned:** The leak and subsequent public exposure of these activities have led to significant introspection within these agencies. The discussion reflects a keen interest in learning from the incident to prevent future compromises and enhance the security of cyber operations.
- **Importance of High-Quality Threat Intelligence:** The discussion also underscores the value of high-quality threat intelligence, as demonstrated by Kaspersky's report, which played a crucial role in uncovering these activities. The agencies recognize the need to understand and mitigate the implications of such intelligence findings on national security.

#### 8) Thoughts

- **Collaborative Nature of U.S. Cyber Operations:** it emphasizes that U.S. cyber operations are not the domain of any single agency. Instead, they involve collaboration across various intelligence agencies, including the NSA and the CIA. This collaborative approach is typical of complex cyber operations which require a range of skills and resources that no single agency could effectively manage alone.
- **Role of CIA's IOC:** The CIA's Information Operations Center (IOC) is highlighted as a significant player in the activities attributed to the Equation Group. The IOC's involvement suggests that the operations of the Equation Group are more broadly based within the U.S. intelligence community than previously thought.

- **Misattribution and Misunderstandings:** the challenges and potential inaccuracies involved in attributing cyber activities to specific groups or agencies. Due to the clandestine nature of intelligence efforts and the intricate technicalities of cyber warfare, pinpointing responsibility accurately is exceedingly difficult. Consequently, there is a tendency to oversimplify matters by attributing all advanced cyber operations to the NSA.
  - **Public Perception and Media Simplification:** The criticism of media and public discourse often centers on their tendency to oversimplify the narrative surrounding cyber operations by exclusively attributing them to the NSA. This oversimplification fails to acknowledge the complex reality of inter-agency collaboration and the distributed nature of cyber intelligence and warfare capabilities.
  - **Importance of a Broader View:** It necessitates a more sophisticated comprehension of how the U.S. government conducts cyber operations. Acknowledging the involvement of various agencies beyond the NSA is essential for a thorough grasp of U.S. capabilities and strategies in cyberspace.
- D. Conclusion*
- **Identification of the Equation Group:** The Equation Group is identified as a highly sophisticated and advanced persistent threat, primarily linked to the NSA's Tailored Access Operations (TAO) unit. This group has been active in cyber espionage and cyber warfare, utilizing complex tools and techniques to infiltrate a wide range of targets globally.
  - **Impact of Leaks:** The leaks by Shadow Brokers in 2016 revealed significant details about the Equation Group's operations, including the use of sophisticated tools like Bvp47. These leaks confirmed the group's connection to the NSA and exposed the extensive reach of their cyber operations, affecting over 287 targets in 45 countries.
  - **Technical Sophistication:** The Equation Group's tools, such as Bvp47, demonstrated advanced capabilities in network attack, equipped with 0day vulnerabilities. Their operations were characterized by a high degree of covertness and technical sophistication, making them a dominant force in national-level cyberspace confrontations.
  - **Global Impact and Victims:** The global impact of the Equation Group's activities was vast, with victims across various countries, indicating the strategic and widespread nature of their cyber operations. This included the use of victims' systems as jump servers for further attacks, highlighting the strategic depth of their operations.



# **CHOOSING SECURE AND VERIFIABLE TECHNOLOGIES**



#### A. Introduction

The document "Choosing Secure and Verifiable Technologies" provides comprehensive guidance for organizations on procuring digital products and services with a focus on security from the design phase through the lifecycle of the technology.

Document emphasizes the critical importance of selecting technologies that are inherently secure to protect user privacy and data against the increasing number of cyber threats. It outlines the responsibility of customers to evaluate the security, suitability, and associated risks of digital products and services. It advocates for a shift towards products and services that are secure-by-design and secure-by-default, highlighting the benefits of such an approach, including enhanced resilience, reduced risks, and lower costs related to patching and incident response.

- **Secure-by-Design and Secure-by-Default:** the necessity for technologies to be designed and developed with security is a foundational element, ensuring that products are secure from the outset with minimal need for additional configurations.
- **Procurement Process:** a two-stage procurement approach – pre-purchase and post-purchase assessments includes evaluating the security features of the product, the manufacturer's transparency, and the ongoing support and updates provided by the manufacturer.
- **Manufacturer Considerations:** Organizations are advised to assess the manufacturer's commitment to security, including their ability to provide transparent information about the product's security features and vulnerabilities. Manufacturers should adhere to practices like publishing complete and timely CVEs.
- **Risk Management:** the importance of continuous risk management, both during the procurement process and

throughout the lifecycle of the product or service includes regular updates and patches from the manufacturer to address new vulnerabilities.

- **Supply Chain Risks:** there is a focus on managing risks associated with the supply chain, emphasizing the need for organizations to ensure that their suppliers adhere to secure-by-design principles.
- **Security Incident Management:** it covers the necessity for effective security incident and event management (SIEM) and security orchestration, automation, and response (SOAR) integration to manage and mitigate potential security incidents.
- **End of Life and Post-Purchase Considerations:** the need for clear policies regarding the end of life of products and services, including secure data disposal and transitioning to new technologies.
- **Regulatory and Compliance Issues:** organizations are encouraged to ensure that the products and services comply with relevant regulations and standards, which may vary depending on the industry and type of data handled.

#### B. Audience

The document is targeted at a broad audience within the realm of digital technology procurement and manufacturing.

- **Organizations that procure and leverage digital products and services:** This encompasses a wide range of entities known as procuring organizations, purchasers, consumers, and customers. These organizations are the main focus of the guidance provided in the document, aiming to enhance their decision-making process in procuring digital technologies.
- **Manufacturers of digital products and services:** The document also addresses the manufacturers of digital technologies, providing them with insights into secure-by-design considerations. This is intended to guide manufacturers in developing technologies that meet the security expectations of their customers.

Key personnel encouraged to read and utilize this guidance include:

- **Organization Executives and Senior Managers:** Leaders who play a crucial role in decision-making and strategy formulation for their organizations.
- **Cyber Security Personnel and Security Policy Personnel:** Individuals responsible for ensuring the security of digital technologies within their organizations.
- **Product Development Teams:** Those involved in the creation and development of digital products and services, ensuring these offerings are secure by design.
- **Risk Advisers and Procurement Specialists:** Professionals who advise on risk management and specialize in the procurement process, ensuring that

digital technologies procured do not pose undue risks to the organization.

The document is designed to be comprehensive, encouraging all audiences to read it in its entirety for several purposes:

- To inform organizations about secure-by-design considerations for the procurement of digital products and services, leading to better-informed assessments and decisions.
- To inform manufacturers about secure-by-design considerations for their products and services, aiming to increase the development of secure technologies. It provides manufacturers with key security questions and expectations they can anticipate from their customers.

The document emphasizes that it is not a checklist for perfect digital procurement outcomes but rather a guide to assist procuring organizations in making informed, risk-based decisions within their unique operational contexts. It acknowledges the uniqueness of every organization in its structure and approach to procurement and suggests that not every item in the document may be relevant to every organization. Additionally, it may be necessary for organizations to consider other factors not covered in the document, which may be unique to their specific situation or the industry or region in which they operate.

#### C. "Secure-by-Design" Concept

The concept of "Secure-by-Design" (SbD) is a proactive and security-centric approach adopted by software manufacturers during the development of digital products and services. This approach necessitates a deliberate alignment of cybersecurity objectives at all organizational levels involved in the manufacturing process.

- **Proactive Security Integration:** SbD requires that security considerations are integrated from the very beginning of the product development process, rather than being added as an afterthought. This integration occurs across all stages of design, development, and deployment.
- **Purposeful Alignment of Cybersecurity Goals:** The approach demands that cybersecurity goals are aligned with business objectives and product design from the outset. This alignment ensures that security measures are embedded within the architecture of the product or service.
- **Consideration of Cyber Threats:** Manufacturers must consider potential cyber threats during the initial stages of product design. This foresight allows for the implementation of mitigative measures early in the development process, reducing the likelihood of vulnerabilities in the final product.
- **Core Value of User Privacy and Data Protection:** The primary aim of SbD is to safeguard user privacy and data. By designing products with fewer vulnerabilities, manufacturers enhance the security of user data against unauthorized access and potential breaches.

- **Guidance for Procuring Organizations:** Understanding the principles and practices of SbD is crucial for organizations that procure digital products and services. This knowledge helps them make informed decisions, ensuring that the products they acquire are built with security as a foundational element

#### D. Shifting the Balance of Cybersecurity Risk

The document "Choosing Secure and Verifiable Technologies" relates to another whitepaper "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default", led by the Cybersecurity and Infrastructure Security Agency (CISA), is a collaborative effort aimed at guiding technology manufacturers in enhancing the security of their products. This publication is significant as it represents an international endeavor to mitigate exploitable vulnerabilities in technology utilized by both government and private sector organizations. The whitepaper is supported by a coalition of global security agencies, including CISA, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and international partners from Australia, Canada, New Zealand, the United Kingdom, Germany, and the Netherlands, among others.

##### 1) Founding Principles

- **Take Ownership of Customer Security Outcomes:** Manufacturers are encouraged to prioritize the security of their customers by integrating security considerations from the initial stages of product development. This principle emphasizes the importance of designing products that are inherently secure, thereby reducing the risk of cyber threats to end-users.
- **Embrace Radical Transparency and Accountability:** This principle advocates for manufacturers to be open and transparent about the security features of their products. It calls for the disclosure of potential vulnerabilities and the steps taken to mitigate them, fostering a culture of accountability.
- **Lead from the Top:** The whitepaper underscores the critical role of senior executives in embedding security into the corporate culture. It suggests that leadership should champion security as a core business goal, ensuring that it is considered a priority throughout the product development lifecycle.

##### 2) Impact and Implementation

The whitepaper provides a roadmap for manufacturers to develop products that are secure by design and default, offering protection against prevalent cyber threats without requiring additional configurations or costs for end-users. It suggests that adopting these principles can shift the burden of security from consumers to manufacturers, reducing the likelihood of security incidents resulting from common issues like misconfigurations or delayed patching.

The document highlights the need for a strategic focus on software security, urging manufacturers to make difficult trade-offs and investments, including adopting programming languages that mitigate common vulnerabilities and prioritizing security over appealing but potentially risky features.

#### E. Categories of Digital Products and Services

The various categories of digital products and services emphasize the importance of understanding these categories to ensure secure procurement and usage.:

##### 1) Software

- **General Definition:** Software encompasses all types of programs and applications, including operating systems and embedded systems.
- **Proprietary Software:** This is software developed by manufacturers and distributed under specific licensing or purchasing agreements. It often has restrictions such as user limits and prohibitions on resale or modification.
- **Open-source Software (OSS):** OSS includes software with source code that is freely available under an open license, allowing anyone to view, use, study, or modify it. Managed by a community of volunteers, OSS facilitates rapid product development due to its collaborative nature.

##### 2) Embedded Software and Firmware

- **Embedded Software:** This software controls embedded systems designed for specific functions within larger systems, typically constrained by available processing resources and designed for real-time operations.
- **Firmware:** A type of embedded software, firmware is permanently stored in a device's non-volatile memory and provides low-level control over the device's hardware components.

##### 3) Software Bill of Materials (SBOM)

- **Functionality:** An SBOM lists the software components or libraries that make up a software package. It applies to all software types, including proprietary, OSS, embedded, and firmware.
- **Utility:** SBOMs help manufacturers and consumers identify the components and their versions within a product, facilitating the monitoring of updates and vulnerabilities. SBOMs are typically machine-readable to support automated monitoring and reporting.

##### 4) Hardware

- **Scope:** Hardware includes any physical device designed to process, store, or transmit data. This category covers network devices (e.g., firewalls, routers), storage devices, and servers.
- **Hardware Bill of Materials (HBOM):** An HBOM describes the physical components that make up a hardware device. It is crucial for understanding the materials used in hardware and assessing potential supply chain risks.

##### 5) Internet of Things (IoT)

IoT generally falls under hardware and includes devices and sensors that connect to the internet to exchange data and provide functionality. This category includes consumer products, medical devices, and operational technologies.

##### 6) Cloud Services

Cloud service providers offer on-demand computing resources, including infrastructure, platform, storage, networking, and processing services. Security considerations like those for software and hardware procurement apply here.

##### 7) Software as a Service (SaaS)

SaaS allows consumers to use software without the need to install or manage it themselves. It reduces management overheads and infrastructure costs and can be offered under various agreements, including free access.

##### 8) Managed Service Providers (MSPs)

**Role:** MSPs provide specialized services to help organizations manage, secure, and optimize their cloud infrastructure. Services include cloud infrastructure management, security, and data backup and recovery, allowing clients to focus on core business activities.

#### F. External procurement considerations

External procurement considerations are divided into the pre-purchase and post-purchase phases to ensure secure and informed decisions when acquiring digital products and services.

##### 1) Pre-purchase phase

The pre-purchase phase focuses on several key areas to ensure that organizations make informed and secure choices when procuring digital products and services.

##### a) Transparency and Reporting

- Organizations should verify the transparency of the information provided by manufacturers, which can include industry reports, independent testing, and security feature updates.
- Manufacturers are expected to notify customers of any vulnerabilities found and provide guidance on mitigations, ideally at no extra cost.
- The publication of complete and timely Common Vulnerabilities and Exposures (CVEs) is crucial for maintaining transparency.

##### b) Secure-by-Default

- Products should be secure out of the box, requiring minimal security setup from the consumer to operate safely.
- Secure-by-default features might include multifactor authentication and security logging, with default settings configured to the highest security level.

##### c) Security Requirements

- Organizations must define and understand their specific security needs to ensure that procured products meet these requirements.
- Considerations include encryption standards and identity credentials management.

##### d) Supply Chain Risk Management

- Assessing the security of a manufacturer's supply chain is vital as vulnerabilities can be inherited by the procuring organization.

- Manufacturers should have a supply chain risk management plan to address potential risks.
- e) *Open-source Software Usage*
  - The use of open-source software (OSS) should be managed carefully to avoid security risks.
  - Manufacturers should ensure OSS components are regularly updated and secure.
- f) *Data Sharing and Sovereignty*
  - Understanding what data will be shared, how it will be used by the manufacturer, and ensuring compliance with data protection laws are critical.
  - Considerations include the geographical locations where data is stored and processed.
- g) *Development Process*
  - Organizations should verify that manufacturers follow secure development practices.
  - This includes assessing whether products are developed in a secure environment and adhere to relevant standards.
- h) *Geopolitical Risks*
  - Manufacturers should be aware of and manage geopolitical risks that could impact their products and services.
  - This includes understanding the political stability of the regions where they operate and their supply chains.
- i) *Regulated Industries*

Products must be assessed for compliance with specific regulatory requirements relevant to the industry in which they are used.
- j) *Manufacturer Access*
  - Assessing the need for and security of any manufacturer access to the organization's systems is crucial.
  - This includes both remote and physical access controls.
- k) *Insider Threat*
  - Consider potential risks from insiders within the manufacturer's organization who could harm the procuring organization.
  - Controls such as robust hiring practices and monitoring should be in place.
- l) *Open Standards*
  - The use of open standards promotes interoperability and reduces the risk of vendor lock-in.
  - Organizations should verify that products adhere to these standards.
- m) *Connected Systems*

Understanding all systems that the product will connect to is essential to assess potential risks and manage them effectively.
- n) *Product Value*

Evaluating the overall value of a product, including its cost, expected lifespan, and the security posture it brings to the organization, is crucial for making informed procurement decisions

#### 2) Post-purchase phase

The post-purchase phase addresses several critical aspects of managing digital products and services after acquisition. These aspects are crucial for ensuring ongoing security, compliance, and operational efficiency.

##### a) Risk Management

- Organizations must ensure continuous risk management to address new and evolving threats.
- Regular assessments and updates are necessary to adapt to changes in the threat landscape and to maintain the security integrity of the technology throughout its lifecycle.
- Security Incident Event Management and Security Orchestration, Automation, and Response (SIEM and SOAR)
- Integration of SIEM and SOAR solutions is vital for detecting and rectifying malicious activities effectively.
- These tools require detailed logs from applications to function optimally, and manufacturers should work with SIEM and SOAR providers to ensure their products are logging sufficient information.

##### b) Maintenance and Support

- Organizations must verify that manufacturers adhere to maintenance and support commitments stated during the procurement phase.
- This includes providing timely updates and patches as well as support for addressing any vulnerabilities discovered post-purchase.

##### c) Contracts, Licensing, and Service Level Agreements

- It is crucial to ensure that all contractual obligations and service level agreements are upheld by the manufacturer.
- Organizations should regularly review these agreements to confirm ongoing compliance and to address any changes that may affect service quality or security.

##### d) Loosening Guides

- Manufacturers should provide guides that detail the configuration settings that users can change within a product.
- These guides should explain the security implications of altering configurations from their default settings and suggest possible compensating security measures.

##### e) End of Life

- The end-of-life process for a product should be managed carefully to avoid security risks associated with unsupported or outdated technologies.

- Organizations should plan for the secure disposal or transition of the product at the end of its life, ensuring that all data is appropriately handled and that the product is decommissioned in a manner that maintains security

#### G. Internal Procurement Considerations

Internal procurement considerations are divided into three phases: pre-purchase, purchasing, and post-purchase. Each phase addresses specific aspects that organizations need to consider internally when procuring digital products and services.

##### 1) Pre-purchase phase

The pre-purchase phase focuses on ensuring that the internal aspects of an organization align with the procurement of digital products and services. This phase involves consultations and evaluations across various departments within the organization to ascertain that the product or service being considered meets the organizational needs and security standards.

###### a) Senior Management

- **Risk Assessment and Approval:** Senior management is responsible for establishing the organizational risk threshold and approving the procurement based on a comprehensive risk assessment. This includes understanding the potential risks associated with the product or service and ensuring these are within acceptable limits.
- **Incident Response Plan Inclusion:** It is crucial for senior management to ensure that the product or service is included in the organization's incident response plan, indicating preparedness for potential security incidents.

###### b) Policy

- **Policy Compliance:** The procurement must be evaluated against existing policies to ensure there are no conflicts. This includes checking that the level of risk associated with the product or service does not exceed the organization's accepted risk thresholds.
- **Regulatory and Legislative Compliance:** The product or service must meet all relevant logging and auditing requirements, which may be dictated by legislative or regulatory standards. This ensures compliance and aids in the smooth integration of the product or service into the organization's operations.

###### c) Infrastructure and Security

- **Security Control Compatibility:** The existing security controls, frameworks, or standards that the organization adheres to must be compatible with the new product or service. A security impact assessment should be completed to evaluate this compatibility.
- **Threat Modeling:** A thorough threat model should be developed to identify relevant threats and risks, ensuring that these are managed to an acceptable level. This helps in understanding how the product or service will fit into the existing infrastructure and what adjustments might be necessary.

###### d) Product Owner

- **Business Needs and Risk Tolerance:** The product owner must assess whether the product meets the

business needs without exceeding the organization's risk tolerance. This includes evaluating the security classification level that the purchase needs to meet.

- **Contract and Risk Mitigation:** The proposed contract should cover an acceptable level of risk and include appropriate risk mitigation measures. The product owner plays a crucial role in ensuring that the contract terms are suitable and that a risk mitigation plan is established

##### 2) Purchasing phase

The purchasing phase involves critical evaluations and decisions that ensure the alignment of the procurement process with organizational goals and security requirements.

###### a) Senior Management

- **Decision Making and Risk Acceptance:** Senior management is responsible for finalizing the procurement decisions. This includes accepting any residual risks identified during the procurement process and ensuring these risks are within the organization's risk tolerance.
- **Contract Approval:** Senior management plays a crucial role in reviewing and approving the final contracts, ensuring that all terms meet the organization's requirements and that the contracts provide adequate protection and value.

###### b) System Administration

- **Verification of Technical Specifications:** **System administrators** are tasked with verifying that the technical specifications of the procured products or services meet the organization's requirements. This includes confirming that all system configurations, integrations, and customizations are correctly implemented.
- **Security and Compliance Checks:** They ensure that the new systems comply with existing security policies and standards. System administrators also play a role in setting up and configuring new systems to maintain security and operational efficiency.

###### c) Infrastructure and Security

- **Integration and Compatibility:** This area focuses on ensuring that the new procurement integrates seamlessly with the existing infrastructure without compromising security or performance. It involves conducting detailed compatibility checks and planning for any necessary infrastructure upgrades.
- **Ongoing Security Assessments:** Post-integration, it is crucial to continuously assess the security posture of the integrated systems to identify and mitigate any emerging risks promptly.

###### d) Product Owner

- **Alignment with Business Needs:** The product owner ensures that the procured products or services align with the business needs and strategic goals. This includes verifying that the features and capabilities of the product meet the specified requirements.

- **Management of Product Lifecycle:** They are also responsible for overseeing the lifecycle of the product from procurement to deployment and beyond, ensuring that the product continues to meet the needs of the organization as those needs evolve
- 3) *Post-purchase phase*
  - The post-purchase phase involves ensuring that the procured digital products and services continue to align with the organization's security, operational, and strategic goals. This phase requires ongoing assessments and management practices to address any emerging risks or changes in the organization's or product's environment.
  - a) *Senior Management*
    - **Continuous Risk Acceptance and Review:** Senior management should establish a process for the continuous or periodic acceptance and review of product risks. This includes ensuring that the product's risks are managed on the organization's risk register and that system security plans and business continuity plans are updated and accepted.
    - **Legacy Technology Management:** Senior management must also address the risks associated with legacy technology, ensuring these are documented and managed appropriately within the organization's risk framework.
  - b) *System Administration*
    - **Monitoring for Security Updates:** System administrators are responsible for setting up monitoring and notification systems for patches, CVEs, and product updates, including those related to the full supply chain. This ensures that the organization remains aware of and can respond to new vulnerabilities or updates.
    - **Integration with SIEM and SOAR:** The product should be integrated within the organization's SIEM (Security Information and Event Management) system, and if applicable, SOAR (Security Orchestration, Automation, and Response) capabilities should be provisioned. This integration aids in the detection and response to security incidents.
    - **Data Management Procedures:** Procedures for data management, including disposal, editing, and backup, should be established and followed to protect the integrity and confidentiality of data.
  - c) *Infrastructure and Security*
    - **Periodic Review of Authorizations:** The organization should periodically review authorizations and privilege accounts to ensure that access controls remain appropriate and secure.
    - **Review of Manufacturer's Security Attestations:** Security attestations provided by the manufacturer should be periodically reviewed for updates to ensure that the product continues to meet the required security standards.
    - **Management of Legacy and New Technologies:** The organization should have a roadmap or support plan for managing both legacy and new technologies, ensuring that security and operational risks are addressed.
  - d) *Product Owner*
    - **Manufacturer Adherence to Claims:** The product owner should verify that the manufacturer continues to adhere to the security and operational claims made during the purchase phase.
    - **Periodic Contract Reviews:** Contracts and service level agreements with the manufacturer should be periodically reviewed to ensure ongoing compliance and to address any changes in the organization's needs or the product's performance.
    - **Risk Assessment of Changes:** Any changes to the product, including updates or configuration changes, should be risk assessed to ensure they do not introduce new vulnerabilities or compromise security.
    - **Development of Continuity and Security Plans:** The product owner should ensure that business continuity plans and system security plans are developed and maintained, addressing both regulatory and legislative requirements



# **EUROPOL CYBERCRIME TRAINING COMPETENCY FRAMEWORK 2024**



**Abstract – This document presents a comprehensive analysis of the "Europol Cybercrime Training Competency Framework 2024," a pivotal resource aimed at enhancing the capabilities of law enforcement, judiciary, and academic institutions in combating cybercrime. This analysis delves into various critical aspects of the framework, including the identification of essential skill sets for key actors involved in cybercrime mitigation, the development process of the framework, and its strategic context within the broader EU Strategy to tackle Organized Crime 2021-2025.**

**This document serves as a valuable resource for enhancing the preparedness and response of law enforcement and judiciary personnel to cybercrime. It underscores the importance of continuous training and capacity building in the fight against cybercrime, thereby contributing to the security and resilience of digital spaces across the European Union and beyond.**

#### A. Introduction

The Europol Cybercrime Training Competency Framework 2024 encompasses a wide range of documents related to cybercrime training, competency frameworks, strategies, and legislation. These materials (as compilation by Europol) collectively aim to enhance the capabilities of law enforcement, judiciary, and other stakeholders in combating cybercrime effectively.

Key aspects to be explored include the framework's approach and scope, detailing the functional competences required by law enforcement authorities and the judiciary, and the flexibility and adaptability of the framework to different organizational structures. Additionally, the analysis will cover the specific roles outlined within the framework, such as heads of cybercrime units, team leaders, general criminal investigators, and specialized cybercrime experts, among others.

- **Europol Cybercrime Training Competency Framework:** outlines the necessary skill sets for various roles within law enforcement and judiciary to combat cybercrime effectively. It emphasizes the importance of digital forensics, network investigation, programming, and specific cybercrime knowledge among other skills.

- **European Union Initiatives:** Documents highlight the efforts by the European Union to strengthen cybercrime fighting capabilities through EC3 (European Cybercrime Centre) and collaborations with entities like CEPOL and ECTEG. These efforts include training, operational support, and the development of a harmonized legal framework to tackle cybercrime.
- **Global and National Strategies:** Various sources discuss the global and national strategies for cybercrime legislation and capacity building. The ITU Toolkit for Cybercrime Legislation and the National Cybercrime Strategy Guidebook by Interpol provide guidelines for developing effective cybercrime laws and strategies. These strategies emphasize the need for harmonization of laws, capacity building for criminal justice authorities, and international cooperation.
- **Training and Education:** The importance of training and education in cybercrime investigation is underscored across several sources. The National Cybercrime Training Centre (CyTrain) and the Cybercrime Investigation Body of Knowledge (CIBOK) offer specialized training and certifications for law enforcement officers and other stakeholders. These training programs cover various aspects of cybercrime investigation, including digital forensics, intelligence analysis, and management.
- **Collaboration and Information Sharing:** The need for collaboration among law enforcement agencies, private sector, academia, and international organizations is a recurring theme. Effective combat against cybercrime requires a multidisciplinary approach, sharing of best practices, and leveraging expertise from different sectors.
- **Legislation and Legal Frameworks:** Several documents discuss the challenges and recommendations for updating legal frameworks to effectively criminalize and prosecute cybercrimes. The need for laws that keep pace with technological advancements and facilitate international cooperation is highlighted.
- **Capacity Building and Resource Allocation:** The sources emphasize the need for building capacity among law enforcement and judiciary through training, provision of technical resources, and development of specialized units to handle cybercrime cases. This includes addressing gaps in skills, knowledge, and technology.

#### B. Framework

- **Purpose of the Framework:** The framework aims to identify the required skill sets for key actors involved in combating cybercrime. It serves as a guide for law enforcement authorities, judiciary, and academic institutions to understand the competencies needed to effectively tackle the evolving threat of cybercrime.
- **Development Process:** The framework was developed following a multi-stakeholder consultation process. This included contributions from various European bodies

such as the European Union Agency for Law Enforcement Training (CEPOL), European Cybercrime Training and Education Group (ECTEG), Eurojust, European Judicial Cybercrime Network (EJCN), and representatives nominated by the European Union Cybercrime Task Force (EUCTF).

- **Strategic Context:** The renewed framework is part of the European Commission's action plan aimed at enhancing the capacity and capabilities of law enforcement authorities in digital investigations. This is aligned with the EU Strategy to tackle Organized Crime for the period 2021-2025.
- **Scope and Limitations:** The framework focuses on the unique skills pertinent to cybercrime investigations and handling of digital evidence. It does not cover all skills required for the roles described but emphasizes those specific to cybercrime. The framework is not an exhaustive list of skills nor an endorsement of a specific unit structure or employee profiles. It is intended for strategic capacity building within the organizational structures of law enforcement authorities.
- **Flexibility and Adaptation:** Depending on the organizational structure and staffing, the roles and corresponding skill sets outlined in the framework could be combined or outsourced to specialized units such as criminal analysis and forensics.
- **Functional Competences:** The framework identifies the essential functional competences required by law enforcement authorities to effectively combat cybercrime. It emphasizes the specific skills needed for cybercrime investigations and handling digital evidence, rather than general law enforcement skills.
- **Non-Exhaustive Skill List:** The framework does not provide an exhaustive list of skills but focuses on those uniquely pertinent to cybercrime investigations. This approach allows for targeted development of competencies that are most critical in the cybercrime context.
- **Strategic Capacity Building:** The framework is intended as a tool for strategic capacity building within law enforcement and judicial institutions. It aims to enhance the competencies that are crucial for the effective handling of cybercrime cases.
- **Exclusion of General Skills:** General law enforcement training, management skills, and soft skills are not included in the framework. This exclusion ensures that the framework remains focused on the specialized skills necessary for cybercrime interventions.
- **Development Process:** The framework was developed through a comprehensive process that included online questionnaires, an in-person workshop, and a review of responses from involved stakeholders. This collaborative approach ensured that the framework reflects the current needs and future requirements of law enforcement and academic institutions.

- **Competency Matrix:** The competency matrix is a central element of the framework, depicting the necessary roles, skill sets, and desired skill levels for practitioners. This matrix serves as a visual guide to understanding the specific competencies required across different roles within cybercrime investigations.
- **Role Descriptions:** Detailed descriptions of the main functions and skill sets for various roles are provided throughout the framework. These roles include heads of cybercrime units, team leaders, general criminal investigators, cybercrime analysts, and specialized experts among others. Each role is tailored to address specific aspects of cybercrime and digital evidence handling.
- **Skill Sets and Levels:** The framework outlines specific skill sets required for each role and the desired levels of proficiency. These skill sets include digital forensics, network investigation, programming, and cybercrime legislation, among others. The framework emphasizes the importance of having tailored skills that are directly applicable to the challenges of cybercrime.

### C. Roles

- **Heads of Cybercrime Units:** These individuals are responsible for overseeing cybercrime units, making informed decisions about cybercrime cases, coordinating resources, and prioritizing policing activities. They need to have a comprehensive understanding of the unit's capabilities and provide necessary training and tools for staff. Effective communication and relationship management skills, especially in English, are essential for interacting with international stakeholders.
- **Team Leaders:** Team leaders manage cybercrime investigations within their specific areas. They supervise ongoing investigations, coordinate with senior management, and ensure their team is equipped with the necessary training and tools. Like heads of units, they require practical experience in evaluating operational activities and strong communication skills.
- **General Criminal Investigators:** These investigators increasingly encounter cyber elements in various crimes. They need a fundamental understanding of the digital world, including how to handle electronic evidence at crime scenes and utilize open-source intelligence (OSINT) effectively.
- **Cybercrime Analysts:** Analysts are involved in collecting and analyzing data to produce actionable intelligence and strategic insights. They need to process large amounts of data from diverse sources and translate these into concise reports. Sharing information with wider audiences and participating in strategic meetings are also part of their role.
- **Cybercrime Investigators:** These are specialized investigators with a deeper understanding of data extraction and online information acquisition. They lead

cybercrime investigations and are involved in training other trainers within the law enforcement community.

- **Specialized Cybercrime Experts:** These experts have specialized knowledge in specific areas of cybercrime, such as OSINT, Dark Web, cryptocurrencies, and IoT devices. They provide operational support in investigations and need to keep their skills updated through peer exchanges at national and international levels.
- **Digital Forensic Examiners (Investigators):** These professionals focus on identifying, recovering, and analyzing digital evidence. They are familiar with various operating systems, forensic tools, and have skills in scripting and programming. They prepare evidence for advanced decryption tasks and report their findings.
- **Cyber-attack Response Experts:** These experts handle the technical response to cyber-attacks, cooperating with various stakeholders like Computer Emergency Response Teams (CERTs) and IT departments. They are responsible for preserving digital evidence and ensuring its integrity for judicial processes.
- **First Responders:** First responders are usually the initial law enforcement officers at the scene of a cyber incident. They need basic knowledge of digital forensics and cybercrime, and their responsibilities include identifying and securing electronic evidence according to national regulations and best practices.
- **Trial and Appeal Judges:** Judges dealing with cybercrime cases need to integrate cyber evidence effectively into the judicial process. They should acquire and maintain updated knowledge of cybercrime and electronic evidence.
- **Prosecutors and Investigative Judges:** These legal professionals direct criminal investigations involving cyber elements, assess the collection of electronic evidence, and present cases in court. They require a basic understanding of the digital world and the ability to use intelligence from various sources, including OSINT, to complement their investigations

#### D. Skills

- **Digital Forensics:** Involves identification, preservation, acquisition, validation, analysis, interpretation, documentation, and presentation of electronic evidence from digital sources. Key areas include live data forensics, OS forensics, file system forensics, mobile forensics, network forensics, IoT forensics, cloud forensics, and cryptography.
- **Network Investigation and Administration:** Pertains to understanding network functions, conducting investigative activities within networks, and analyzing traffic data to identify indicators of compromise. Skills include network administration, live network data acquisition, network forensic and traffic data analysis,

and expertise in cyber-crime investigations and evidence retention.

- **Programming and Scripting:** Utilized for building information systems and automating tasks to support investigations and data analysis. Important programming languages include Python, JavaScript, Java, and C++, among others. Skills also cover backend, frontend development, and full-stack development.
- **Reporting and Presenting Cybercrime Investigative Data:** Encompasses documentation, note-taking, and final report writing across various report types. It emphasizes the importance of structured reporting that is factual, credible, and admissible in court. Presentation skills include synthesizing information and adapting complex technical topics for non-technical audiences.
- **Analysis and Visualization:** Involves applying data analysis techniques to describe, illustrate, and summarize cybercrime data to find patterns, trends, and actionable knowledge plus data gathering, research design, statistical methods, visualization best practices, and ethical considerations in handling crime data.
- **Cybercrime Legislation:** Relates to understanding legislation governing cyber-criminal activity, including national legislation on cybercrime and electronic evidence, privacy laws, GDPR, EU regulations on data retention, and international court rulings.
- **General Cybercrime Knowledge:** Covers information related to cyber-enabled and cyber-dependent crime, cybercrime trends, threats, and modi operandi, as well as an understanding of cybersecurity.
- **Specific Cybercrime Knowledge:** Refers to unique skills obtained through specialized training in specific areas of cybercrime. Areas include OSINT, Dark Web, blockchains and cryptocurrencies, intrusion analysis and incident response, ethical hacking, threat intelligence, and malware analysis and reverse engineering.
- **Crime Scene Management & Electronic Evidence Handling:** Pertains to standards and best practices in identifying and seizing electronic evidence at crime scenes. Skills include collecting, packaging, transferring, and storing devices that may contain electronic evidence, as well as conducting on-the-scene interviews and supporting victims.
- **Cybercrime Investigative Techniques:** Consists of skills required for a cybercrime investigation, such as intelligence gathering techniques, processing and interpreting data, tracing suspects online and offline, online undercover work, cybercriminal interrogation/questioning, and investigation risk management

Read more: [Boosty](#) | [Sponsr](#) | [TG](#)



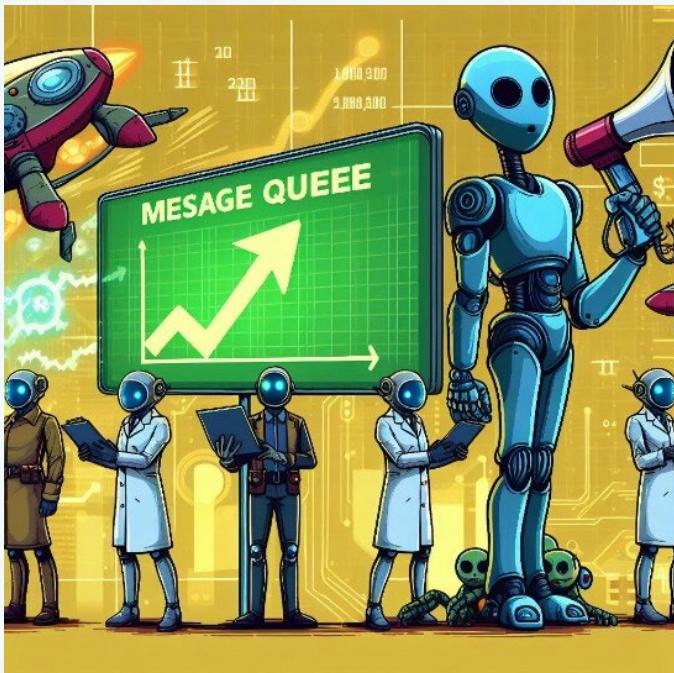
STARRY SECURITY



# **SECTION: RESEARCH**



**MARKET INSIGHTS.  
SIMPLE SOLUTIONS ARE  
JUST TOO CHEAP,  
SPENDING MORE IS  
ALWAYS BETTER**



**Abstract –** This document provides a comprehensive analysis of the Message Queue Brokers market, focusing on various critical aspects that influence its growth and development. The document offers a high-quality summary of the current state and prospects of the Message Queue Brokers market. This analysis is particularly valuable for security professionals and other specialists across various industries, providing insights into the secure and efficient management of distributed systems. The detailed examination of performance, security, and technological trends equips stakeholders with the knowledge needed to make informed decisions and enhance their operational capabilities.

#### A. Introduction

Message brokers are essential components in modern distributed systems, enabling seamless communication between applications, services, and devices. They act as intermediaries that validate, store, route, and deliver messages, ensuring reliable and efficient data exchange across diverse platforms and programming languages. This functionality is crucial for maintaining the decoupling of processes and services, which enhances system scalability, performance, and fault tolerance. Message brokers support various messaging patterns, including point-to-point and publish/subscribe, catering to different use cases such as financial transactions, real-time notifications, and IoT data streaming.

The message broker market is experiencing significant growth, driven by the increasing adoption of cloud-based solutions and the need for robust, scalable communication infrastructures in distributed systems. Major players in this market include Kinesis, Cisco IoT, Solace, RabbitMQ, Apache Kafka, ApacheMQ, IBM MQ, Microsoft Azure Service Bus, and Google Cloud IoT, each offering unique capabilities and serving a wide range of industries from financial services to healthcare and smart cities. These brokers are deployed globally, with substantial user bases in regions like North America, Europe, and Asia-Pacific, reflecting their critical role in enabling modern, interconnected applications.

#### B. Combined data

- **Market Share:** The percentage of the market each broker holds in the queuing, messaging, and background processing category.
- **Number of Users:** The total number of companies or devices using the broker.
- **Corporate Users:** The number of enterprise customers using the broker.
- **Revenue Distribution:** The distribution of companies using the broker based on their revenue.
- **Geographical Coverage:** The percentage of users based in different regions.

#### Broker's market share and user base

Broker	Market Share	Number of Users	Corporate Users
RabbitMQ	28.24%	15,851	14,651
Apache Kafka	39.73%	22,244	22,244
Apache ActiveMQ	5.79%	9,604	9,604
IBM MQ	7.12%	4,060	4,060
Microsoft Azure Service Bus	3.84%	12,870	4,609
EMQX	N/A	20,000+	500+
HiveMQ	N/A	20,000+	500+
PubNub	N/A	330M devices	500+
ThingsBoard	N/A	Thousands	500+
AWS IoT	N/A	718	718
Azure IoT	14.90%	1,396	1,396
Google Cloud IoT	18.65%	1,790	1,790
Cisco IoT	9.52%	129	129
Solace	5.33%	133	133
Amazon Kinesis	1.20%	216	216

#### Broker's revenue and geo coverage

Broker	Customer	Revenue Distribution	Geographical Coverage (%)
Rabbit MQ	Currys, Beckman Coulter	< \$50M: 39%, \$50M-\$1B: 16%, > \$1B: 40%	US: 46.15%, India: 9.72%, UK: 9.70%
Apache Kafka	LinkedIn, Uber, Netflix	< \$50M: 52%, \$50M-\$1B: 18%, > \$1B: 24%	US: 51.91%, India: 12.95%, UK: 8.28%
Apache Active MQ	Infosys, Fujitsu, Panasonic	< \$50M: 24%, \$50M-\$1B: 43%, > \$1B: 33%	US: 47%, UK: 6%, India: 6%
IBM MQ	American Airlines, Aflac	< \$50M: 39%, \$50M-\$1B: 16%, > \$1B: 40%	US: 59.39%, UK: 8.70%, India: 8.67%
Microsoft Azure Service Bus	Infosys, Fujitsu, Panasonic	< \$50M: 40%, \$50M-\$1B: 17%, > \$1B: 39%	US: 48.02%, UK: 14.97%, India: 8.98%
EMQX	IoT sector companies	N/A	50+ countries
HiveMQ	Fortune 500 companies	N/A	US: 60%

PubNub	US companies	N/A	Global
Things Board	IoT sector companies	N/A	50+ countries
AWS IoT	Global companies	N/A	US: 52.12%, India: 13.26%, UK: 8.84%
Azure IoT	Global companies	N/A	US: 47.72%, India: 14.04%, UK: 8.73%
Google Cloud IoT	Global companies	N/A	US: 48.77%, India: 16.58%, Germany: 6.39%
Cisco IoT	Infosys, Cisco Systems, Wipro, AT&T, Cognizant	< \$50M: 25%, \$50M-\$1B: 17%, > \$1B: 47%	US: 50%, India: 9%
Solace	Large enterprises in finance, telecom, manufacturing	< \$50M: 16%, \$50M-\$1B: 29%, > \$1B: 49%	US: 38.18% France: 10.91% Canada: 10%
Amazon Kinesis	Siemens, Microsoft, Oracle, Cisco	< \$50M: 25%, \$50M-\$1B: 15%, > \$1B: 60%	US: 61.78% India: 10.47% UK: 8.38%

### C. Broker's vulnerability coverage

#### 1) RabbitMQ

- **Windows-Specific Binary Planting Vulnerability:** RabbitMQ versions 3.8.x prior to 3.8.7 are prone to a Windows-specific binary planting security vulnerability that allows for arbitrary code execution. An attacker with write privileges to the RabbitMQ installation directory and local access on Windows could carry out a local binary hijacking (planting) attack and execute arbitrary code.
- **Denial of Service (DoS) via "X-Reason" HTTP Header:** RabbitMQ versions 3.7.x prior to 3.7.21 and 3.8.x prior to 3.8.1 contain a web management plugin that is vulnerable to a denial-of-service attack. The "X-Reason" HTTP Header can be leveraged to insert a malicious Erlang format string that will expand and consume the heap, resulting in the server crashing.
- **Cross-Site Scripting (XSS) Vulnerabilities:** Several forms in the RabbitMQ management UI are vulnerable to XSS attacks. This includes versions prior to v3.7.18 and RabbitMQ for PCF versions 1.15.x prior to 1.15.13, 1.16.x prior to 1.16.6, and 1.17.x prior to 1.17.3.
- **MQTT Authentication Bypass:** An issue was discovered in RabbitMQ 3.x before 3.5.8 and 3.6.x before 3.6.6 where MQTT connection authentication with a username/password pair succeeds if an existing username is provided but the password is omitted from the connection request.
- **Sensitive Information Exposure:** The metrics-collection component in RabbitMQ for Pivotal Cloud Foundry (PCF) 1.6.x before 1.6.4 logs command lines of failed commands, which might allow context-dependent attackers to obtain sensitive information by reading the log data.

- **Denial of Service via AMQP 1.0 Client Connection Endpoint:** RabbitMQ all versions prior to 3.8.16 are prone to a DoS vulnerability due to improper input validation in the AMQP 1.0 client connection endpoint.

- **TLS/DTLS Authentication Bypass (CVE-2022-37026):** A critical vulnerability identified as CVE-2022-37026 originates from a bug in Erlang OTP and may allow a malicious actor to bypass the authentication process and impersonate other users when the server is configured to use TLS or DTLS authentication.

#### 2) Apache Kafka

- **Denial of Service (DoS) via InternalTopicManager:** A bug in the InternalTopicManager prior to 2.1.0 can cause a DoS attack. When a topic is marked for deletion but not yet deleted, the Broker gives inconsistent information, causing the client to enter a loop polling for topic metadata, leading to a DoS condition.
- **Timing Attack Vulnerability (CVE-2021-38153):** Some components in Apache Kafka 2.0.0 to 2.8.0 use Arrays.equals to validate a password or key, which is vulnerable to timing attacks, making brute force attacks more likely to succeed.
- **Plaintext Secrets Exposure (CVE-2019-12399):** The Kafka 2.0.0 to 2.3.0 Connect REST API may expose plaintext secrets in the tasks endpoint when configured with one or more config providers.
- **Out-of-Memory (OOM) via Snappy Compression (CVE-2023-34455):** A vulnerability in the snappy-java library used by Kafka 0.8.0 to 3.5.0 can cause an Out-of-Memory (OOM) condition, leading to a DoS attack when a malicious payload compressed using snappy-java is decompressed by Kafka.
- **Remote Code Execution (RCE) via Kafka Connect (CVE-2023-25194):** Unsafe deserialization in the Kafka Connect 2.3.0 to 3.3.2 REST API can allow a remote authenticated attacker to execute arbitrary code or cause a DoS attack.
- **Denial of Service via Improper Input Validation (CVE-2022-34917):** Improper input validation can allow a remote attacker to allocate large amounts of memory on brokers, resulting in a DoS condition.
- **Java Deserialization Vulnerability (CVE-2023-34040):** A deserialization attack in Spring for Apache Kafka 3.0.9 and earlier, 2.9.10 and earlier can be exploited if unusual configuration is applied, allowing an attacker to construct a malicious serialized object.

#### 3) ApacheMQ

- **CVE-2023-46604: Remote Code Execution (RCE):** This critical vulnerability allows remote attackers to execute arbitrary shell commands by exploiting serialized class types in the OpenWire protocol. The flaw is due to the failure to properly validate throwable class types when OpenWire commands are unmarshalled. Affected Versions: Apache ActiveMQ 5.18.x before 5.18.3, Apache ActiveMQ 5.17.x before

- 5.17.6, Apache ActiveMQ 5.16.x before 5.16.7, All versions before 5.15.16
- **CVE-2022-41678: Deserialization Vulnerability:** This vulnerability in Jolokia allows authenticated users to perform remote code execution (RCE) by exploiting deserialization of untrusted data.
  - **CVE-2020-13947: Cross-Site Scripting (XSS):** XSS vulnerabilities in the WebConsole allow remote attackers to inject arbitrary web scripts or HTML.
  - **CVE-2020-13920: JMX MITM Vulnerability:** A man-in-the-middle (MITM) vulnerability in JMX allows remote attackers to intercept and manipulate communications.
  - **CVE-2016-3088: Remote File Upload and Execution:** Fileserver web application in Apache ActiveMQ allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.
  - **CVE-2015-1830: Path Traversal Leading to RCE:** A path traversal vulnerability in the fileserver upload/download functionality allows remote attackers to create JSP files in arbitrary directories, leading to remote code execution.
  - **CVE-2014-3576: Remote Unauthenticated Shutdown of Broker (DoS):** This vulnerability allows remote attackers to shut down the broker without authentication, leading to a denial of service (DoS).
- 4) *IBM MQ*
- **CVE-2022-27780 and CVE-2022-30115:** These vulnerabilities reside within the libcurl library used by IBM MQ 9.2 LTS, 9.1 LTS, 9.0 LTS, 9.2 CD, and 9.1 CD. CVE-2022-27780 allows an attacker to bypass security restrictions using a specially crafted host name in a URL. CVE-2022-30115 is a HSTS check bypass flaw that could be exploited to obtain sensitive information over clear-text HTTP.
  - **CVE-2023-26285: Denial of Service (DoS):** IBM MQ 8.0, 9.0-9.1 LTS, 9.2 LTS, 9.3 LTS, 9.1 CD, 9.2 CD, and 9.3 CD.is vulnerable to a DoS attack caused by an error processing invalid data from a compromised client.
  - **CVE-2022-43902: Denial of Service (DoS) via PCF or MQSC Messages:** An authenticated attacker with sufficient MQ permissions can send specially crafted PCF or MQSC messages to execute a DoS attack. Affected Versions: IBM MQ 9.1-9.3 LTS, 9.1-9.3 CD.
  - **CVE-2023-45177: Denial of Service (DoS) via MQ Clustering Logic:** IBM MQ Appliance 9.2 LTS, 9.3 LTS, and 9.3 CD.is vulnerable to a DoS attack due to an error within the MQ clustering logic.
  - **CVE-2022-21624 and CVE-2022-21626: Java Runtime Environment Vulnerabilities:** Multiple vulnerabilities in the IBM Runtime Environment Java Technology Edition, Version 8, which is shipped with IBM MQ. CVE-2022-21624 allows an unauthenticated attacker to update, insert, or delete data. CVE-2022-21626 allows an unauthenticated attacker to cause a DoS. Affected Versions: IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.1 CD, 9.2 CD, and 9.3 CD.
  - **CVE-2023-22081 and CVE-2023-5676: Java SE and Eclipse OpenJ9 Vulnerabilities:** CVE-2023-22081 is an unspecified vulnerability in Java SE related to the JSSE component, allowing a remote attacker to cause low availability impact. CVE-2023-5676 in Eclipse OpenJ9 can cause an infinite busy hang or segmentation fault when a shutdown signal is received before JVM initialization. Affected Versions: IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, and 9.3 CD.
  - **CVE-2020-13947: Cross-Site Scripting (XSS):** XSS vulnerabilities in the WebConsole allow remote attackers to inject arbitrary web scripts or HTML.
  - **CVE-2020-13920: JMX MITM Vulnerability:** A MITM vulnerability in JMX allows remote attackers to intercept and manipulate communications.
  - **CVE-2016-3088: Remote File Upload and Execution:** Fileserver web application in Apache ActiveMQ allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.
  - **CVE-2015-1830: Path Traversal Leading to RCE:** A path traversal vulnerability in the fileserver upload/download functionality allows remote attackers to create JSP files in arbitrary directories, leading to remote code execution.
  - **CVE-2014-3576: Remote Unauthenticated Shutdown of Broker (DoS):** This vulnerability allows remote attackers to shut down the broker without authentication, leading to a denial of service (DoS).
- 5) *Microsoft Azure Service Bus*
- **Denial of Service (DoS) Vulnerability (MS14-042):** A vulnerability in Microsoft Service Bus for Windows Server could allow a remote authenticated attacker to create and run a specially crafted script, leading to a denial of service (DoS) condition.
  - **Denial of Service (DoS) via Resource Exhaustion:** Azure Service Bus may become unavailable during DoS attacks aimed at overwhelming its resources or disrupting its operation. This can occur due to network issues, service outages, resource exhaustion, configuration errors, security concerns, software bugs, or data center failures.
  - **Remote Code Execution (RCE) in Power Platform Connectors:** A RCE vulnerability was discovered in Power Platform Connectors that allowed access to cross-tenant data. This issue was fixed by rebuilding the serialization binder to enforce stricter type allow lists.
  - **Data Encryption and Security Risks:** While Azure Service Bus supports encryption in transit and at rest, there are risks associated with data exfiltration, unauthorized data movements, and unauthorized access.

Proper logging and monitoring are essential to detect and respond to these risks.

## 6) EMQX

- CVE-2021-33175: Denial of Service (DoS):** A vulnerability in EMQX versions prior to 4.2.8 allows for a denial of service (DoS) attack due to excessive memory consumption when handling malformed MQTT messages.
- CVE-2023-46604: Directory Traversal:** A directory traversal vulnerability in the emqx\_sn plugin of EMQX v4.3.8 allows attackers to execute a directory traversal via uploading a crafted .txt file.
- Heap Buffer Overflow Vulnerabilities:** Multiple heap buffer overflow vulnerabilities exist in NanoMQ 0.21.7, a component of EMQX, which can be exploited to cause a denial of service (DoS) via specially crafted hexstreams.
- Use-After-Free Vulnerability:** A use-after-free vulnerability in NanoMQ v0.21.2 allows attackers to cause a denial of service via crafted MQTT messages.
- Null Pointer Dereference:** A null pointer dereference vulnerability in the topic\_filtern function in mqtt\_parser.c in NanoMQ 0.21.7 allows attackers to cause a denial of service.
- Username Enumeration:** EMQX Dashboard v3.0.0 is affected by a username enumeration vulnerability in the "/api/v3/auth" interface, allowing attackers to determine if a given username is valid.
- Denial of Service via Memory Consumption:** EMQX Broker versions prior to 4.2.8 are vulnerable to a denial-of-service attack due to excessive memory consumption when handling untrusted inputs.
- TLS Protocol Session Renegotiation Vulnerability:** A vulnerability related to TLS protocol session renegotiation on port 8084 (TCP over SSL).

## 7) HiveMQ

- CVE-2020-13821: Reflected Cross-Site Scripting (XSS):** A vulnerability in the HiveMQ Broker Control Center (version 4.3.2) allows for reflected cross-site scripting (XSS). This can be exploited by an attacker to execute arbitrary web scripts or HTML in the context of the user's browser.
- Denial of Service (DoS) via Resource Exhaustion:** HiveMQ can be vulnerable to DoS attacks that aim to exhaust broker resources such as disk, RAM, or CPU. This can occur if an attacker sends many heavy messages or exploits the broker's handling of message queues.
- SlowITe Attack:** SlowITe attack exploits the MQTT protocol's Keep-Alive parameter, allowing an attacker to set an arbitrary value that keeps the connection open for an extended period, leading to a DoS condition.

- Heap-Based Buffer Overflow:** vulnerability in the HiveMQ Broker can be exploited to cause a denial of service (DoS) or potentially execute arbitrary code.

## 8) Pubhub

- CVE-2023-26154: Insufficient Entropy:** This vulnerability in the PubNub package (versions before 6.19) involves insufficient entropy in the generation of cryptographic keys, which can be exploited by an attacker to brute-force the encryption.
- Reflected Cross-Site Scripting (XSS):** A vulnerability in the platform allows for reflected XSS attacks. This can be exploited by an attacker to execute arbitrary web scripts or HTML in the context of the user's browser.
- Persistent Connection Vulnerability:** There are concerns about the security of PubNub's persistent connections through port 80 or port 443. While PubNub claims these connections are safe, vulnerabilities could still exist if not properly managed.
- Security Vulnerabilities in Insteon Hub:** Multiple vulnerabilities were discovered in the Insteon Hub, which uses PubNub for communication. These vulnerabilities range from RCE to DoS attacks.
- Vulnerabilities in Custom Implementations:** Custom implementations of PubNub, especially those using older versions or insecure config, may be vulnerable to various attacks, including MITM and data exfiltration.

## 9) Thingsboard

- CVE-2022-45608: Vertical Privilege Escalation:** A vulnerability in ThingsBoard IoT platform version 3.4.2 allows a low-privileged user (CUSTOMER\_USER) to escalate their privileges to become an Administrator (TENANT\_ADMIN) or system administrator (SYS\_ADMIN) using a simple POST request with the platform's REST API.
- CVE-2023-26462: Insecure Secret Key Management:** A vulnerability allows attackers to escalate privileges within the system by manipulating JSON Web Tokens (JWTs). The static default secret key used for signing JWTs can be exploited to re-sign modified tokens, granting unauthorized access. Affected Versions: Prior to version 3.4.2.
- CVE-2021-42751: Stored Cross-Site Scripting (XSS):** A stored XSS vulnerability in ThingsBoard version 3.3.1 allows attackers to execute arbitrary JavaScript code by injecting a script payload into the description field of a rule node.
- CVE-2023-45303: Server-Side Template Injection:** ThingsBoard before version 3.5 is vulnerable to server-side template injection if users are allowed to modify an email template. This vulnerability can be exploited to execute arbitrary code on the server.
- CVE-2020-27687: Host Header Injection:** Product before version 3.2 is vulnerable to host header injection

in password-reset emails. This allows an attacker to send malicious links in password-reset emails.

- **CVE-2023-26462: Default Static Key:** The use of a default static key for signing JWTs in ThingsBoard allows attackers to forge valid requests and escalate privileges. Affected Versions: Prior to version 3.4.2.

#### 10) Solace

- **Kernel Vulnerabilities:** Multiple kernel vulnerabilities have been identified and addressed in Solace PubSub+ Event Broker Appliance and Software versions prior to 9.10.0. These vulnerabilities include issues that could lead to denial of service (DoS), privilege escalation, and other security risks. CVE IDs: CVE-2021-26930, CVE-2021-26931, CVE-2021-26932, CVE-2021-27363, CVE-2021-27364, CVE-2021-27365, CVE-2021-28038, CVE-2021-30002, CVE-2019-19060, CVE-2021-28660, CVE-2021-29265, CVE-2021-28964, CVE-2021-28971, CVE-2021-28972, CVE-2021-28688, CVE-2021-29647, CVE-2021-3483, CVE-2021-29154, CVE-2020-25670, CVE-2020-25671, CVE-2020-25672
- **Amazon Linux 2 Vulnerabilities:** Several critical vulnerabilities in Amazon Linux 2, including issues in systemd and the kernel, have been addressed. These vulnerabilities could lead to remote code execution (RCE), denial of service (DoS), and other security risks. CVE IDs: CVE-2018-15686, CVE-2018-16864, CVE-2018-16866, CVE-2018-16888, CVE-2019-20386, CVE-2019-3815, CVE-2019-6454, CVE-2021-33200
- **Apache Log4j Vulnerabilities:** The Apache Log4j vulnerabilities (Log4Shell) allow for remote code execution (RCE) and have been widely publicized. These vulnerabilities affect many systems that use Log4j for logging. CVE IDs: CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2022-23305
- **Spring Framework Vulnerabilities:** Multiple vulnerabilities in the Spring Framework and Spring Cloud could lead to remote code execution (RCE) and other security risks.
- **OpenSSL Vulnerability:** A critical vulnerability in OpenSSL could lead to security risks such as man-in-the-middle (MITM) attacks.
- **XZ Utils Vulnerability:** A vulnerability in XZ Utils was identified, but it was determined that no Solace products were affected.

#### 11) AWS IoT

- **Denial of Service (DoS) via Resource Exhaustion:** AWS IoT can be vulnerable to DoS attacks that aim to exhaust broker resources such as disk, RAM, or CPU. This occurs if an attacker sends many heavy messages or exploits the broker's handling of message queues.
- **Cross-Site Scripting (XSS):** XSS vulnerabilities in the AWS IoT platform can allow attackers to inject

malicious scripts into the context of the user's browser, potentially leading to data theft or further exploitation.

- **Host Header Injection:** AWS IoT before version 3.2 is vulnerable to host header injection in password-reset emails. This allows an attacker to send malicious links in password-reset emails. CVE ID: CVE-2020-27687

#### 12) Azure IoT

- **CVE-2024-27099: Remote Code Execution (RCE) in uAMQP C Library:** A vulnerability in the uAMQP C library used by Azure IoT for communication with Azure Cloud Services. The vulnerability, caused by a "double free" memory error, can lead to RCE
- **CVE-2021-42312, CVE-2021-37222, CVE-2021-42313, CVE-2021-42311: Multiple Critical Vulnerabilities in Azure Defender for IoT:** Multiple vulnerabilities in Azure Defender for IoT, including issues in the password reset mechanism and SQL injection vulnerabilities, allow unauthenticated attackers to gain unauthorized access and potentially RCE.
- **CVE-2019-0741: Information Disclosure in Azure IoT Java SDK:** An information disclosure vulnerability in the Azure IoT Java SDK logs sensitive information, which can be exploited by an attacker to gain access to sensitive data.
- **Host Header Injection:** Azure IoT before version 3.2 is vulnerable to host header injection in password-reset emails. This allows an attacker to send malicious links in password-reset emails. CVE ID: CVE-2020-27687
- **Insecure Secret Key Management:** A vulnerability involving insecure secret key management allows attackers to escalate privileges within the system by manipulating JSON Web Tokens (JWTs). The static default secret key used for signing JWTs can be exploited to re-sign modified tokens, granting unauthorized access. CVE ID: CVE-2023-26462

#### 13) Google Cloud IoT

- **Weak Passwords and Authentication Issues:** A significant portion of attacks on Google Cloud Platform (GCP) instances, including IoT deployments, are due to weak passwords or no passwords at all. In 48% of the analyzed cases, weak or absent passwords were the primary cause of successful attacks.
- **Vulnerabilities in Cloud-Server Software:** In 26% of the cases, vulnerabilities in the cloud-server software were exploited by attackers. These vulnerabilities can lead to unauthorized access and control over the IoT devices and data.
- **Server or Application Misconfiguration:** Misconfigurations in servers or applications accounted for 12% of the successful attacks that can expose sensitive data and services to unauthorized access.
- **Password or Access Key Leaks:** In 4% of the cases, password or access key leaks were the cause of

successful attacks due to authentication data is uploaded to public repositories like GitHub.

- **CVE-2023-44487: HTTP/2 Rapid Reset DDoS Vulnerability:** A high-severity vulnerability in the HTTP/2 protocol, known as the "Rapid Reset" technique, can be exploited to launch large-scale DDoS attacks. This vulnerability affects web applications, services, and APIs that use HTTP/2.
- **CVE-2023-52620: Privilege Escalation in Linux Kernel:** A vulnerability in the Linux kernel lead to privilege escalation on Container-Optimized OS and Ubuntu nodes. This vulnerability can be exploited to gain unauthorized access and control over the system.
- **CVE-2023-5736: Container Escape Vulnerability:** A vulnerability in the runc container runtime, used by Docker and Kubernetes, allows an attacker to escape the container and execute code on the host system.
- **GhostToken Vulnerability:** A vulnerability in Google Cloud Platform (GCP) allowed attackers to modify and hide OAuth applications, creating a stealthy backdoor to any Google account. This vulnerability, referred to as GhostToken, could be exploited to retrieve account tokens and access the victim's data.

#### 14) Kinesis IoT

- **Cross-Site Scripting (XSS):** XSS vulnerabilities in the AWS IoT platform can allow attackers to inject malicious scripts into the context of the user's browser, potentially leading to data theft or further exploitation.
- **Denial of Service (DoS) via Resource Exhaustion:** AWS Kinesis can be vulnerable to DoS attacks that aim to exhaust broker resources such as disk, RAM, or CPU. This can occur if an attacker sends many heavy messages or exploits the broker's handling of message queues.
- **Host Header Injection:** AWS IoT before version 3.2 is vulnerable to host header injection in password-reset emails. This allows an attacker to send malicious links in password-reset emails. CVE ID: CVE-2020-27687

#### 15) Cisco Internet of Things

- **CVE-2022-20773: Cross-Site Scripting (XSS) in Cisco IoT Control Center:** A vulnerability in the web-based management interface of Cisco IoT Control Center could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input.
- **CVE-2023-20198: Privilege Escalation in Cisco IOS XE:** A critical flaw in the IOS XE web interface can be exploited by remote, unauthenticated attackers for privilege escalation. This vulnerability allows threat actors to create high-privileged accounts on targeted devices and take complete control of the system.

- **CVE-2023-31242 and CVE-2023-34998: Authentication Bypass in OAS Platform:** Multiple vulnerabilities in the Open Automation Software (OAS) Platform prior version 19.00.0000, which is used in industrial IoT environments, can be exploited to bypass authentication, leak sensitive information, and overwrite files. These vulnerabilities allow attackers to gain unauthorized access and control over the system.
- **CVE-2023-34317: Improper Input Validation in OAS Platform:** An improper input validation bug in the user creation functionality of the OAS Platform prior version 19.00.0000 allows attackers to add a user with the username field containing an SSH key, potentially gaining access to the underlying system.
- **CVE-2023-34353: Information Disclosure in OAS Platform:** An authentication bypass vulnerability in the OAS Platform prior version 19.00.0000 allows an attacker to perform network sniffing to capture the protobuf containing admin credentials and then decrypt sensitive information.
- **CVE-2020-7592: Data Integrity Compromise in Siemens Devices:** A vulnerability impacting various Siemens devices and components where data integrity can be compromised.

#### D. Broker market coverage

##### 1) RabbitMQ

RabbitMQ is a robust and widely adopted message broker with a significant market share in the queueing, messaging, and background processing market. It is used by thousands of companies globally, including major corporations like Alcatel-Lucent, University of California - San Diego, and Beckman Coulter. RabbitMQ's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in financial services, healthcare, e-commerce, telecommunications, and manufacturing. The competitive landscape includes other major players like Apache Kafka, IBM MQ, and Apache ActiveMQ, but RabbitMQ's extensive feature set and proven performance give it a strong position in the market.

##### a) Market Share & Geographical Distribution

- RabbitMQ holds a significant market share in the queueing, messaging, and background processing market, with approximately 28.24%.
- **Global Presence:** RabbitMQ is used in 93 countries worldwide.
- **United States:** 46.15% of RabbitMQ's customers are based in the United States.
- **India:** 9.72% of RabbitMQ's customers are based in India.
- **United Kingdom:** 9.70% of RabbitMQ's customers are based in the United Kingdom.

##### b) Growth Drivers

- **Resource Management:** RabbitMQ's ability to manage resources effectively, such as memory and CPU, ensures high performance and reliability, which drives its adoption in various industries.
- **Advanced Routing:** RabbitMQ supports complex routing mechanisms, making it suitable for diverse messaging scenarios, which enhances its market appeal.
- **Monitoring and Metrics:** Comprehensive monitoring capabilities help in maintaining system health and performance, which is crucial for enterprise applications.
- c) *Number of Users*
  - **Total Companies:** Over 35,000 companies use RabbitMQ globally.
  - **Clusters:** Approximately 9,000 RabbitMQ clusters are operating worldwide.
  - **Connected Devices:** RabbitMQ connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.
- d) *Notable Corporate Users*
  - **Alcatel-Lucent:** Uses RabbitMQ for various messaging needs.
  - **University of California - San Diego:** Implements RabbitMQ in its systems.
  - **Beckman Coulter:** Utilizes RabbitMQ for its operations.
  - **Zalando, WeWork, Wunderlist, Bloomberg:** These companies rely on RabbitMQ for their microservice-based architectures.
  - **Capital One, Ford, State Farm, United Airlines, Zurich Insurance:** Major corporations using RabbitMQ for secure and reliable messaging.
- e) *Customer Distribution by Company Size*
  - **20-49 Employees:** 3,520 companies.
  - **100-249 Employees:** 3,034 companies.
  - **1,000-4,999 Employees:** 1,723 companies.
  - **Median Number of Queues:** 26 (largest number of queues: 124,400).
  - **Median Number of Users:** 2 (largest number of users: 62,245).
  - **Median Number of Policies:** 3 (largest number of policies: 2,550).
  - **Median Number of Exchanges:** 9 (largest number of exchanges: 191,465).
  - **Median Number of Bindings:** 28 (largest number of bindings: 142,516).
  - **Median Number of Vhosts:** 2 (largest number of vhosts: 1,954).

#### f) *Scalability*

- **Scalability:** RabbitMQ supports clustering, high availability, and load balancing, making it scalable for various enterprise needs.
- **High Throughput:** RabbitMQ can handle over 1 billion messages per day depending on the configuration.
- **Consistent Hashing:** RabbitMQ can be scaled effectively using consistent hashing, which distributes the load evenly across multiple nodes, ensuring optimal performance and resilience.

#### g) *Industry Adoption*

- **Financial Services:** RabbitMQ is extensively used in the financial sector for secure and reliable messaging.
- **Healthcare:** Used by top healthcare companies for data integration and messaging.
- **E-commerce:** Companies like Zalando and WeWork use RabbitMQ for order processing, tracking, and fulfillment.
- **Telecommunications:** Employed by major telecom companies for data integration and real-time processing.
- **Manufacturing:** Used by large manufacturing companies for data streaming and analytics.

#### h) *Competitive Landscape*

- **RabbitMQ vs. Apache Kafka:** Kafka holds a larger market share and is preferred for high-throughput, low-latency applications, while RabbitMQ is often used for traditional messaging systems with strong transactional support.
- **RabbitMQ vs. IBM MQ:** IBM MQ is favored for its reliability and exactly-once message delivery, whereas RabbitMQ is chosen for its flexibility and ease of use.
- **RabbitMQ vs. Apache ActiveMQ:** ActiveMQ is another competitor with a smaller market share, used for simpler messaging needs compared to RabbitMQ's enterprise-grade capabilities.

### 2) *Apache Kafka*

Apache Kafka is a leading message broker and stream processing platform with a dominant market share and widespread adoption across various industries. It is used by thousands of companies, including over 80% of the Fortune 100, for real-time data processing, analytics, and integration. Kafka's scalability, high throughput, and robust architecture make it a preferred choice for large-scale data streaming applications. The competitive landscape includes other messaging systems like RabbitMQ, Apache Pulsar, and IBM MQ, but Kafka's extensive ecosystem and proven performance give it a significant edge.

#### a) *Market Share & Geographical Distribution*

- Apache Kafka commands a dominant 70% market share in the message broker and stream processing market.
- **United States:** 51.91% of Apache Kafka's customers.
- **India:** 12.95% of Apache Kafka's customers.

- **United Kingdom:** 8.28% of Apache Kafka's customers.
- b) *Growth Drivers*
- **High Throughput and Low Latency:** Kafka's ability to handle high throughput with low latency makes it ideal for real-time data streaming and analytics, driving its popularity among large enterprises.
- **Scalability:** Kafka's distributed architecture allows it to scale horizontally, handling large volumes of data efficiently, which is a significant growth driver.
- **Ecosystem Integration:** Kafka's extensive ecosystem, including built-in stream processing and integration with various data sources and sinks, enhances its utility and adoption
- c) *Number of Users*
- **Total Companies:** Over 22,240 companies use Apache Kafka globally.
- **Fortune 100:** More than 80% of the Fortune 100 companies use Kafka.
- d) *Notable Corporate Users*
- **American Express:** Uses Kafka for real-time data processing.
- **Cardinal Health:** Implements Kafka for handling large-scale data streams.
- **Cisco:** Utilizes Kafka for its data integration needs.
- **Shopify:** Employs Kafka for stream processing and data analytics.
- **LinkedIn:** Processes 7 trillion messages daily using Kafka.
- **Uber:** One of the largest deployments of Kafka, handling data exchange between users and drivers.
- **Netflix:** Tracks activity for over 230 million subscribers using Kafka.
- **Goldman Sachs, Target, Intuit:** Among other major corporations using Kafka.
- e) *Company Size Distribution:*
- **20-49 Employees:** 4,394 companies.
- **100-249 Employees:** 4,149 companies.
- **1,000-4,999 Employees:** 2,838 companies.
- f) *Revenue Distribution:*
- **Small (<\$50M):** 52% of companies using Kafka.
- **Large (>\$1000M):** 24% of companies using Kafka.
- **Medium (\$50M-\$1000M):** 18% of companies using Kafka.
- g) *Scalability*
- **Scalability:** Kafka's distributed architecture allows it to handle increased data loads as a business grows,

ensuring robustness and reliability even as demand increases.

- **High Throughput:** Kafka can deliver messages at network-limited throughput using a cluster of machines with latencies as low as 2ms.
- **Large Scale:** Kafka can scale production clusters up to a thousand brokers, trillions of messages per day, petabytes of data, and hundreds of thousands of partitions.

#### *h) Industry Adoption*

- **Financial Services:** Used by companies like ING, PayPal, and JPMorgan Chase for fraud detection, real-time analytics, and customer handling.
- **E-commerce:** Companies like Shopify and Article use Kafka for order processing, tracking, and fulfillment.
- **AdTech:** Utilized for real-time marketing data aggregation and analytics.
- **Telecommunications:** Employed by major telecom companies for data integration and real-time processing.
- **Manufacturing:** Used by 10 out of 10 of the largest manufacturing companies for data streaming and analytics.

#### *i) Competitive Landscape*

- **Apache Kafka vs. RabbitMQ:** Kafka has a higher market share and is preferred for high-throughput, low-latency applications, while RabbitMQ is often used for traditional messaging systems.
- **Apache Kafka vs. Apache Pulsar:** Kafka holds a dominant 70% market share compared to Pulsar's 30%, with Kafka being more mature and having a larger ecosystem of tools and libraries.
- **Apache Kafka vs. IBM MQ:** Kafka is favored for its scalability and real-time processing capabilities, whereas IBM MQ is often used for enterprise messaging with strong transactional support.

#### *3) ApacheMQ*

Apache ActiveMQ is a widely used message broker with a significant market share in the enterprise application integration space. It is used by thousands of companies globally, including major corporations like Red Hat, The Apache Software Foundation, and eBay. ActiveMQ's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in information technology, computer software, and financial services. The competitive landscape includes other major players like Apache Kafka, RabbitMQ, and IBM MQ, but ActiveMQ's flexibility and support for multiple protocols give it a strong position in the market.

#### *a) Market Share & Geographical Distribution*

- Apache ActiveMQ holds a market share of approximately 4.91% in the Enterprise Application Integration category.

- **United States:** 47% of Apache ActiveMQ's customers are based in the United States.
- **United Kingdom:** 6% of Apache ActiveMQ's customers are based in the United Kingdom.

*b) Growth Drivers*

- **Flexibility and Customization:** ApacheMQ's support for various messaging protocols and its flexibility in deployment options make it a preferred choice for many organizations.
- **Reliability and Persistence:** The ability to ensure message persistence and reliability even in the event of system failures drives its adoption in critical applications.

*c) Number of Users*

- **Total Companies:** Over 9,604 companies use Apache ActiveMQ globally.
- **Current Customers:** Around 3,240 companies have started using Apache ActiveMQ as a queueing, messaging, and background processing tool.

*d) Notable Corporate Users*

- **Red Hat:** Uses Apache ActiveMQ for various messaging needs.
- **The Apache Software Foundation:** Implements Apache ActiveMQ in its systems.
- **Fidelis Cybersecurity:** Utilizes Apache ActiveMQ for its operations.
- **Stack Overflow:** Employs Apache ActiveMQ for message brokering.
- **Infosys Ltd:** A major user of Apache ActiveMQ, based in India.
- **Fujitsu Ltd:** Uses Apache ActiveMQ in Japan.
- **Panasonic Corp:** Another significant user in Japan.
- **eBay Inc.:** Utilizes Apache ActiveMQ in the United States.

*e) Customer Distribution by Company Size*

- **Small Companies (<50 employees):** 24% of Apache ActiveMQ's customers.
- **Medium Companies (50-200 employees):** 43% of Apache ActiveMQ's customers.
- **Large Companies (>1000 employees):** 33% of Apache ActiveMQ's customers.

*f) Revenue Distribution*

- **Small Companies (<\$50M):** 43% of companies using Apache ActiveMQ.
- **Medium Companies (\$50M-\$1000M):** 18% of companies using Apache ActiveMQ.
- **Large Companies (>\$1000M):** 36% of companies using Apache ActiveMQ.

*g) User Statistics*

- **Total Companies:** 9,604 companies use Apache ActiveMQ.
- **Employee Range:** Most companies using Apache ActiveMQ have between 50-200 employees.
- **Revenue Range:** Many companies using Apache ActiveMQ have revenues between \$10M-\$50M.

*h) Scalability*

- **Scalability:** Apache ActiveMQ supports clustering, high availability, and load balancing, making it scalable for various enterprise needs.
- **High Availability:** ActiveMQ can be configured for high availability using shared storage or network replication.
- **Performance:** ActiveMQ Artemis, the next-generation broker, offers better performance and scalability compared to the classic version.

*i) Industry Adoption*

- **Information Technology and Services:** 28% of Apache ActiveMQ's customers are in this industry.
- **Computer Software:** 16% of Apache ActiveMQ's customers are in this industry.
- **Financial Services:** 6% of Apache ActiveMQ's customers are in this industry.

*j) Competitive Landscape*

- **Apache Kafka:** Holds a 39.80% market share and is a major competitor to Apache ActiveMQ.
- **RabbitMQ:** Holds a 28.24% market share and is another significant competitor.
- **IBM MQ:** Holds a 7.20% market share.
- **Realtime Framework:** Holds a 5.17% market share.
- **Microsoft Azure Service Bus:** Holds a 3.84% market share.

*4) IBM MQ*

IBM MQ is a robust and widely adopted message broker with a significant market share in the queueing, messaging, and background processing market. It is used by thousands of companies globally, including major corporations like Capital One, Ford, and State Farm. IBM MQ's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in financial services, healthcare, and oil and gas. The competitive landscape includes other major players like Apache Kafka, RabbitMQ, and Apache ActiveMQ, but IBM MQ's reliability and exactly once message delivery give it a strong position in the market.

*a) Market Share & Geographical Distribution*

- IBM MQ holds a market share of approximately 7.20% in the queueing, messaging, and background processing market.

- **United States:** 59.39% of IBM MQ's customers are based in the United States.
  - **United Kingdom:** 8.70% of IBM MQ's customers are based in the United Kingdom.
  - **India:** 8.67% of IBM MQ's customers are based in India.
- b) Growth Drivers*
- **Business Process Integration:** IBM MQ's integration with business process management tools provides real-time insights and proactive management, which is a key growth driver.
  - **Security and Compliance:** Enhanced security features and compliance with regulatory standards make IBM MQ a trusted solution for industries with stringent security requirements.

*c) Number of Users*

- **Total Companies:** Over 4,060 companies use IBM MQ globally (~12,870 total).
  - **Current Customers:** IBM MQ is used by 90% of the top 100 global banks, healthcare, airline, and insurance companies.
- d) Notable Corporate Users*
- **Capital One:** Uses IBM MQ for secure and reliable messaging.
  - **Ford:** Implements IBM MQ for data integration and messaging.
  - **State Farm:** Utilizes IBM MQ for its operations.
  - **United Airlines:** Employs IBM MQ for message brokering.
  - **Zurich Insurance:** Uses IBM MQ for secure data exchange.
  - **Infosys Ltd:** A major user of IBM MQ, based in India.
  - **Fujitsu Ltd:** Uses IBM MQ in Japan.
  - **Panasonic Corp:** Another significant user in Japan.
  - **eBay Inc.:** Utilizes IBM MQ in the United States.

*e) Customer Distribution by Company Size*

- **1,000 - 4,999 Employees:** 767 companies.
  - **10,000+ Employees:** 739 companies.
  - **100 - 249 Employees:** 578 companies.
- f) Revenue Distribution*
- **Small Companies (<\$50M):** 39% of companies using IBM MQ.
  - **Medium Companies (\$50M-\$1000M):** 16% of companies using IBM MQ.
  - **Large Companies (>\$1000M):** 40% of companies using IBM MQ.

*g) User Statistics*

- **Total Companies:** 12,870 companies use IBM WebSphere MQ.
- **Employee Range:** Most companies using IBM MQ have between 50-200 employees.
- **Revenue Range:** Many companies using IBM MQ have revenues between \$10M-\$50M.

*h) Scalability*

- **Scalability:** IBM MQ supports clustering, high availability, and load balancing, making it scalable for various enterprise needs.
- **High Availability:** IBM MQ can be configured for high availability using shared storage or network replication.
- **Performance:** IBM MQ offers high performance and stability, ensuring reliable message delivery even under high loads.

*i) Industry Adoption*

- **Financial Services:** IBM MQ is extensively used in the financial sector for secure and reliable messaging.
- **Healthcare:** Used by 70% of the top 10 healthcare companies in the 2022 Forbes Global 2000.
- **Oil and Gas:** Utilized by 80% of the top 10 oil and gas companies in the 2022 Forbes Global 2000.
- **Media:** Employed by 60% of the top 10 media companies in the 2022 Forbes Global 2000.

*j) Competitive Landscape*

- **IBM MQ vs. Apache Kafka:** Kafka holds a larger market share and is preferred for high-throughput, low-latency applications, while IBM MQ is often used for traditional messaging systems with strong transactional support.
- **IBM MQ vs. RabbitMQ:** RabbitMQ has a higher market share and is favored for microservices architectures, whereas IBM MQ is chosen for its reliability and exactly once message delivery.
- **IBM MQ vs. Apache ActiveMQ:** ActiveMQ is another competitor with a smaller market share, used for simpler messaging needs compared to IBM MQ's enterprise-grade capabilities.

*5) Microsoft Azure Service Bus*

Microsoft Azure Service Bus is a robust and widely adopted message broker with a significant market share in the queueing, messaging, and background processing market. It is used by thousands of companies globally, including major corporations like Infosys, Fujitsu, and Panasonic. Azure Service Bus's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in information technology, computer software, and financial services. The competitive landscape includes other major players like Apache Kafka, RabbitMQ, and IBM MQ, but Azure

Service Bus's cloud-native capabilities and strong transactional support give it a strong position in the market.

a) *Market Share & Geographical Distribution*

- Microsoft Azure Service Bus holds a market share of approximately 3.84% in the queueing, messaging, and background processing market.
- **United States:** 48.02% of Microsoft Azure Service Bus's customers are based in the United States.
- **United Kingdom:** 14.97% of Microsoft Azure Service Bus's customers are based in the United Kingdom.
- **India:** 8.98% of Microsoft Azure Service Bus's customers are based in India.

b) *Growth Drivers*

- **Cloud Integration:** Azure Service Bus's seamless integration with other Azure services and its ability to handle cloud-based applications drive its adoption.
- **Auto-scaling:** The ability to automatically scale to handle spikes in throughput ensures consistent performance, which is crucial for dynamic workloads.
- **Security and Reliability:** Robust security measures and reliable message delivery enhance its appeal for enterprise applications

c) *Number of Users*

- **Total Companies:** Over 4,609 companies use Microsoft Azure Service Bus globally.
- **Current Customers:** Around 2,168 companies have started using Microsoft Azure Service Bus as a queueing, messaging, and background processing tool.

d) *Notable Corporate Users*

- **Infosys Ltd:** Uses Microsoft Azure Service Bus for various messaging needs.
- **Fujitsu Ltd:** Implements Microsoft Azure Service Bus in its systems.
- **Panasonic Corp:** Utilizes Microsoft Azure Service Bus for its operations.
- **Blackfriars Insurance Brokers Ltd:** Employs Microsoft Azure Service Bus for message brokering.
- **Blue Cross Blue Shield Association:** Uses Microsoft Azure Service Bus for secure data exchange.
- **ASOS.com:** Utilizes Microsoft Azure Service Bus in the United Kingdom.
- **Avanade:** Uses Microsoft Azure Service Bus in the United States.
- **Verra Mobility:** Employs Microsoft Azure Service Bus for transportation and logistics.

e) *Customer Distribution by Company Size*

- **1,000 - 4,999 Employees:** 392 companies.
- **100 - 249 Employees:** 335 companies.

- **20 - 49 Employees:** 318 companies.

- **10,000+ Employees:** 275 companies.

- **50 - 99 Employees:** 194 companies.

f) *Revenue Distribution*

- **Small Companies (<\$50M):** 40% of companies using Microsoft Azure Service Bus.
- **Medium Companies (\$50M-\$1000M):** 17% of companies using Microsoft Azure Service Bus.
- **Large Companies (>\$1000M):** 39% of companies using Microsoft Azure Service Bus.

g) *User Statistics*

- **Total Companies:** 4,609 companies use Microsoft Azure Service Bus.
- **Employee Range:** Most companies using Microsoft Azure Service Bus have between 50-200 employees.
- **Revenue Range:** Many companies using Microsoft Azure Service Bus have revenues between \$10M-\$50M.

h) *Scalability*

- **Scalability:** Microsoft Azure Service Bus supports clustering, high availability, and load balancing, making it scalable for various enterprise needs.
- **High Availability:** Azure Service Bus can be configured for high availability using shared storage or network replication.
- **Performance:** Azure Service Bus offers high performance and stability, ensuring reliable message delivery even under high loads.

i) *Industry Adoption*

- **Information Technology and Services:** 31% of Microsoft Azure Service Bus's customers are in this industry.
- **Computer Software:** 14% of Microsoft Azure Service Bus's customers are in this industry.
- **Financial Services:** 6% of Microsoft Azure Service Bus's customers are in this industry.

j) *Competitive Landscape*

- **Microsoft Azure Service Bus vs. Apache Kafka:** Kafka holds a larger market share and is preferred for high-throughput, low-latency applications, while Azure Service Bus is often used for traditional messaging systems with strong transactional support.
- **Microsoft Azure Service Bus vs. RabbitMQ:** RabbitMQ has a higher market share and is favored for microservices architectures, whereas Azure Service Bus is chosen for its reliability and exactly-once message delivery.
- **Microsoft Azure Service Bus vs. IBM MQ:** IBM MQ is another competitor with a larger market share, used

for enterprise-grade messaging needs compared to Azure Service Bus's cloud-native capabilities.

#### 6) *EMQX*

EMQX is a robust and widely adopted MQTT broker with a significant market share in the IoT messaging space. It is used by thousands of companies globally, including major corporations like HPE, VMware, and Ericsson. EMQX's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in automotive, manufacturing, energy, and oil & gas. The competitive landscape includes other major players like Mosquitto, NanoMQ, and VerneMQ, but EMQX's extensive feature set and proven performance give it a strong position in the market.

##### a) *Market Share & Geographical Distribution*

- EMQX is a leading MQTT broker with a significant presence in the IoT market. It is recognized as the world's most scalable open-source MQTT messaging platform.
- **Global Presence:** EMQX has a global R&D center in Stockholm and 10+ offices throughout the Americas, Europe, and the Asia-Pacific region.
- **Countries and Regions:** EMQX is used in over 50 countries and regions worldwide.

##### b) *Growth Drivers*

- **IoT Focus:** EMQX's specialization in IoT messaging and its ability to handle large-scale IoT deployments drive its growth in the IoT sector.
- **Scalability:** EMQX's ability to scale horizontally to support millions of concurrent connections is a significant growth driver.

##### c) *Number of Users*

- **Total Users:** EMQX boasts more than 20,000 enterprise users globally.
- **Connected Devices:** EMQX connects over 100 million IoT devices.

##### d) *Notable Corporate Users*

- **Hewlett Packard Enterprise (HPE):** Uses EMQX for its IoT solutions.
- **VMware:** Implements EMQX in its systems.
- **Verifone:** Utilizes EMQX for secure and reliable messaging.
- **SAIC Volkswagen:** Employs EMQX for connected vehicle applications.
- **Ericsson:** Uses EMQX for its IoT infrastructure.

##### e) *Customer Distribution by Company Size*

- **Enterprise Users:** EMQX is trusted by over 500 customers in mission critical IoT scenarios, including well-known brands.

- **Cluster Deployments:** EMQX has over 60,000 cluster deployments globally.

- **GitHub Stars:** EMQX has received over 13,000 stars on GitHub, indicating strong community support and adoption.

- **Downloads:** EMQX has been downloaded over 40 million times.

##### f) *Scalability*

- **Scalability:** EMQX supports up to 100 million concurrent IoT device connections per cluster while maintaining 1 million messages per second throughput and sub-millisecond latency.

- **Cluster Size:** EMQX can scale horizontally with a masterless distributed architecture, ensuring high availability and fault tolerance.

##### g) *Industry Adoption*

- **Automotive:** EMQX is used by over 50 automotive companies, connecting more than 10 million electric and traditional vehicles.
- **Manufacturing:** EMQX empowers Industry 4.0 transformation with seamless connectivity and real-time data transmission from the factory floor to the cloud.
- **Energy & Utilities:** EMQX integrates with energy management and SCADA systems for smart grid management.
- **Oil & Gas:** EMQX consolidates data from oil wells, gateways, and cloud applications to enhance operational efficiency and safety.

##### h) *Competitive Landscape*

- **EMQX vs. Mosquitto:** EMQX offers better scalability and performance, supporting up to 100 million connections compared to Mosquitto's lower capacity.
- **EMQX vs. NanoMQ:** EMQX and NanoMQ both perform well in enterprise-level benchmarks, but EMQX has a larger user base and more extensive feature set.
- **EMQX vs. VerneMQ:** EMQX outperforms VerneMQ in terms of scalability and resource efficiency, making it a preferred choice for large-scale IoT deployments.

#### 7) *HiveMQ*

HiveMQ is a robust and widely adopted MQTT broker with a significant market share in the IoT messaging space. It is used by thousands of companies globally, including major corporations like BMW, Daimler, and Siemens. HiveMQ's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in automotive, manufacturing, energy, and oil & gas. The competitive landscape includes other major players like Mosquitto, NanoMQ, and VerneMQ, but HiveMQ's extensive feature set and proven performance give it a strong position in the market.

##### a) *Market Share & Geographical Distribution*

- HiveMQ is a leading MQTT broker with a significant presence in the IoT market. It is recognized for its scalability and performance, making it a popular choice among enterprises.
- **Global Presence:** HiveMQ has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
- **US Market:** The US market accounts for a significant portion of HiveMQ's revenues, reflecting its widespread adoption in the region.

*b) Growth Drivers*

- **MQTT Protocol Support:** HiveMQ's support for the MQTT protocol, which is widely used in IoT applications, drives its adoption in the IoT market.
- **Enterprise Features:** Features like high availability, security, and integration with enterprise systems make HiveMQ a preferred choice for large-scale IoT deployments.

*c) Number of Users*

- **Total Users:** HiveMQ is used by thousands of companies globally, with a substantial number of enterprise users.
- **Connected Devices:** HiveMQ connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

*d) Notable Corporate Users*

- **BMW:** Uses HiveMQ for connected vehicle applications.
- **Daimler:** Implements HiveMQ in its IoT systems.
- **Deutsche Telekom:** Utilizes HiveMQ for secure and reliable messaging.
- **Liberty Global:** Employs HiveMQ for its IoT infrastructure.
- **Moen:** Uses HiveMQ for smart home applications.
- **Siemens:** Relies on HiveMQ for industrial IoT solutions.
- **ZF:** Uses HiveMQ for automotive IoT applications.

*e) Customer Distribution by Company Size*

- **Enterprise Users:** HiveMQ is trusted by over 500 customers in mission critical IoT scenarios, including well-known brands.
- **Cluster Deployments:** HiveMQ has over 60,000 cluster deployments globally.
- **GitHub Stars:** HiveMQ has received over 13,000 stars on GitHub, indicating strong community support and adoption.
- **Downloads:** HiveMQ has been downloaded over 40 million times.

*f) Scalability*

- **Scalability:** HiveMQ supports up to 100 million concurrent IoT device connections per cluster while maintaining 1 million messages per second throughput and sub-millisecond latency.
- **Cluster Size:** HiveMQ can scale horizontally with a masterless distributed architecture, ensuring high availability and fault tolerance.
- **Benchmark:** HiveMQ has demonstrated the capability to handle 200 million concurrent connections in a large-scale test scenario.

*g) Industry Adoption*

- **Automotive:** HiveMQ is used by over 50 automotive companies, connecting more than 10 million electric and traditional vehicles.
- **Manufacturing:** HiveMQ empowers Industry 4.0 transformation with seamless connectivity and real-time data transmission from the factory floor to the cloud.
- **Energy & Utilities:** HiveMQ integrates with energy management and SCADA systems for smart grid management.
- **Oil & Gas:** HiveMQ consolidates data from oil wells, gateways, and cloud applications to enhance operational efficiency and safety.
- **Logistics:** A large transportation company uses HiveMQ to handle 743.5 million customer tracking requests per day, saving 100 million miles and 10 million gallons of fuel per year.

*h) Competitive Landscape*

- **HiveMQ vs. Mosquitto:** HiveMQ offers better scalability and performance, supporting up to 100 million connections compared to Mosquitto's lower capacity.
- **HiveMQ vs. NanoMQ:** HiveMQ and NanoMQ both perform well in enterprise-level benchmarks, but HiveMQ has a larger user base and more extensive feature set.
- **HiveMQ vs. VerneMQ:** HiveMQ outperforms VerneMQ in terms of scalability and resource efficiency, making it a preferred choice for large-scale IoT deployments.

*8) Pubhub*

PubNub is a robust and widely adopted real-time messaging platform with a significant market share in the real-time data streaming market. It is used by thousands of companies globally, including major corporations like SAP, HPE, and Ericsson. PubNub's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in e-learning, entertainment, healthcare, smart cities, and IoT. The competitive landscape includes other major players like Ably, Pusher, and Firebase, but PubNub's extensive feature set and proven performance give it a strong position in the market.

- a) *Market Share & Geographical Distribution*
  - PubNub holds a significant market share in the real-time messaging and data streaming market. It is recognized for its robust infrastructure and extensive feature set, making it a popular choice among developers and enterprises.
  - **Global Presence:** PubNub has a strong global presence, with data centers distributed across North America, South America, Europe, and Asia.
  - **United States:** A significant portion of PubNub's customers are based in the United States, reflecting its widespread adoption in the region.
  - **Europe and Asia:** PubNub also has a substantial user base in Europe and Asia, supporting a diverse range of applications and industries.
- b) *Growth Drivers*
  - **Ease of Use:** Pubhub's user-friendly interface and ease of integration with various applications drive its adoption among small to medium-sized enterprises.
  - **Cost-Effectiveness:** Competitive pricing and cost-effective solutions make Pubhub an attractive option for businesses looking to implement messaging systems without significant investment.
- c) *Number of Users*
  - **Total Devices:** PubNub serves over 330 million devices globally.
  - **Monthly Transactions:** PubNub handles over 3 trillion API calls per month, demonstrating its capability to manage large-scale real-time data streaming.
- d) *Notable Corporate Users*
  - **SAP:** Uses PubNub for its real-time messaging needs.
  - **Hewlett Packard Enterprise (HPE):** Implements PubNub in its IoT solutions.
  - **VMware:** Utilizes PubNub for secure and reliable messaging.
  - **Verifone:** Employs PubNub for its payment processing systems.
  - **Ericsson:** Uses PubNub for its IoT infrastructure.
  - **Disprz:** Uses PubNub to empower a more knowledgeable workforce through real-time communication.
- e) *Customer Distribution by Company Size*
  - **Enterprise Users:** PubNub is trusted by over 500 enterprise customers in mission-critical scenarios, including well-known brands.
  - **Cluster Deployments:** PubNub has over 60,000 cluster deployments globally.

- **GitHub Stars:** PubNub has received over 13,000 stars on GitHub, indicating strong community support and adoption.
- **Downloads:** PubNub has been downloaded over 40 million times.
- f) *Scalability*
  - **Scalability:** PubNub supports up to millions of concurrent device connections, ensuring high availability and fault tolerance.
  - **High Throughput:** PubNub can handle large volumes of data, making it suitable for high-load environments.
  - **Global Reach:** PubNub operates a globally distributed network with 15 data centers, ensuring low latency and high availability for users worldwide.
- g) *Industry Adoption*
  - **E-Learning:** PubNub is used in interactive classrooms for real-time data updates, chat facilities, and private channels for individual support.
  - **Entertainment:** PubNub supports real-time interactions in online concerts, dating, sporting events, and socializing platforms.
  - **Healthcare:** Used by top healthcare companies for data integration and real-time messaging.
  - **Smart Cities:** PubNub is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.
  - **IoT:** PubNub is extensively used in IoT applications for real-time data streaming and device signaling.
- h) *Competitive Landscape*
  - **PubNub vs. Ably:** Ably offers similar real-time messaging capabilities but PubNub has a more extensive global network and higher reliability guarantees.
  - **PubNub vs. Pusher:** Pusher is another competitor in the real-time messaging space, but PubNub's scalability and feature set give it an edge.
  - **PubNub vs. Firebase:** Firebase provides real-time database capabilities, but PubNub's focus on messaging and data streaming makes it a preferred choice for certain use cases.
- i) *Thingsboard*

ThingsBoard is a robust and widely adopted IoT platform with a significant market share in the IoT messaging space. It is used by thousands of companies globally, including major corporations like CIRCUTOR, OMS, and Ericsson. ThingsBoard's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in smart energy, smart city, smart farming, and smart retail. The competitive landscape includes other major players like AWS IoT, Azure IoT Hub, and Google Cloud IoT, but ThingsBoard's extensive feature set and proven performance give it a strong position in the market.

- a) *Market Share & Geographical Distribution*
  - ThingsBoard is a leading open-source IoT platform with a significant presence in the IoT market. It is widely adopted for its scalability, fault-tolerance, and performance.
  - **Global Presence:** ThingsBoard has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
  - **Countries and Regions:** ThingsBoard is used in over 50 countries and regions worldwide.
- b) *Growth Drivers*
  - **IoT Platform Integration:** Thingsboard's integration with IoT platforms and its ability to handle IoT data efficiently drive its growth in the IoT sector.
  - **Open-Source Flexibility:** Being open-source, Thingsboard offers flexibility and customization, which attracts a wide range of users and developers
- c) *Number of Users*
  - **Total Users:** ThingsBoard is used by thousands of companies globally, with a substantial number of enterprise users.
  - **Connected Devices:** ThingsBoard connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.
- d) *Notable Corporate Users*
  - **CIRCUTOR:** Uses ThingsBoard for energy efficiency and power quality measurement.
  - **OMS:** Implements ThingsBoard in its smart city solutions.
  - **iiOOTE:** Utilizes ThingsBoard for its IoT LPWAN ecosystem.
  - **MAKERS s. r. o.:** Employs ThingsBoard for smart city solutions.
  - **Ericsson:** Uses ThingsBoard for its IoT infrastructure.
  - **Hewlett Packard Enterprise (HPE):** Uses ThingsBoard for its IoT solutions.
  - **VMware:** Implements ThingsBoard in its systems.
  - **Verifone:** Utilizes ThingsBoard for secure and reliable messaging.
  - **SAIC Volkswagen:** Employs ThingsBoard for connected vehicle applications.
- e) *Customer Distribution by Company Size*
  - **Enterprise Users:** ThingsBoard is trusted by over 500 customers in mission critical IoT scenarios, including well-known brands.
  - **Cluster Deployments:** ThingsBoard has over 60,000 cluster deployments globally.
- **GitHub Stars:** ThingsBoard has received over 13,000 stars on GitHub, indicating strong community support and adoption.
- **Downloads:** ThingsBoard has been downloaded over 40 million times.
- f) *Scalability*
  - **Scalability:** ThingsBoard supports up to 100 million concurrent IoT device connections per cluster while maintaining 1 million messages per second throughput and sub-millisecond latency.
  - **Cluster Size:** ThingsBoard can scale horizontally with a masterless distributed architecture, ensuring high availability and fault tolerance.
  - **Benchmark:** ThingsBoard has demonstrated the capability to handle 200 million concurrent connections in a large-scale test scenario.
- g) *Industry Adoption*
  - **Smart Energy:** ThingsBoard is used by companies like CIRCUTOR for energy efficiency and power quality measurement.
  - **Smart City:** ThingsBoard is employed by companies like OMS and iiOOTE for smart city solutions.
  - **Smart Farming:** ThingsBoard supports high-availability deployments on cloud and on-premises data centers using K8S or bare-metal deployments, with production deployments supporting more than 1,000 agriculture sites and 500,000 devices connected.
  - **Smart Retail:** ThingsBoard is used to monitor supermarket assets, browse historical data, and generate alarms based on user-defined thresholds.
  - **Fleet Tracking:** ThingsBoard platform allows tracking vehicles' state and alerts via various sensors, plotting vehicle routes in real-time, and browsing their sensors' reading history using customizable high-quality dashboards.
- h) *Competitive Landscape*
  - **ThingsBoard vs. AWS IoT:** AWS IoT offers a comprehensive suite of IoT services, but ThingsBoard's open-source nature and flexibility make it a preferred choice for many developers and enterprises.
  - **ThingsBoard vs. Azure IoT Hub:** Azure IoT Hub is known for its integration with other Microsoft services, while ThingsBoard offers a more customizable and open-source solution.
  - **ThingsBoard vs. Google Cloud IoT:** Google Cloud IoT provides robust data analytics capabilities, but ThingsBoard's ease of use and flexibility give it an edge in certain scenarios.
- i) *SolaceMQ*

Solace is a robust and widely adopted message broker with a significant market share in the plumbing-and-middleware market. It is used by thousands of companies globally, including

major corporations like SAP, Mercedes-Benz, and the London Stock Exchange. Solace's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in financial services, healthcare, e-commerce, telecommunications, and manufacturing. The competitive landscape includes other major players like Apache Kafka, RabbitMQ, and IBM MQ, but Solace's extensive feature set and proven performance give it a strong position in the market.

*a) Market Share*

- Solace holds a market share of approximately 5.33% in the plumbing-and-middleware market.
- **Global Presence:** Solace has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
- **Countries and Regions:** Solace is used in over 50 countries and regions worldwide.

*b) Growth Drivers*

- **Event Mesh Capabilities:** Solace's event mesh architecture, which enables seamless data exchange across distributed applications, is a key growth driver as organizations adopt event-driven architectures and microservices.
- **Multi-Protocol Support:** Solace's support for various messaging protocols, including MQTT, AMQP, and JMS, allows it to cater to diverse IoT use cases, driving adoption across industries.
- **Cloud-Agnostic Deployment:** Solace's ability to deploy its event brokers across multiple cloud platforms and on-premises environments provides flexibility, enabling growth in hybrid and multi-cloud IoT deployments

*c) Number of Users*

- **Total Companies:** Solace is used by thousands of companies globally, with a substantial number of enterprise users.
- **Connected Devices:** Solace connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

*d) Notable Corporate Users*

- **SAP:** Uses Solace for its event-driven architecture needs.
- **Mercedes-Benz:** Implements Solace in its IoT systems.
- **London Stock Exchange:** Utilizes Solace for secure and reliable messaging.
- **Hewlett Packard Enterprise (HPE):** Uses Solace for its IoT solutions.
- **VMware:** Implements Solace in its systems.
- **Verifone:** Utilizes Solace for secure and reliable messaging.

- **SAIC Volkswagen:** Employs Solace for connected vehicle applications.
- **Ericsson:** Uses Solace for its IoT infrastructure.
- **WeLab Bank:** Uses Solace to support its vision of becoming a leading virtual bank in the region.
- **Standard Chartered Bank Korea:** Collaborates with Solace to design a modern and agile corporate banking platform.
- **Drax Group:** Uses Solace to improve user experience and drive operational efficiencies.
- **RBC Capital Markets:** Relies on Solace for handling unprecedented trading volumes and volatility.
- *e) Customer Distribution by Company Size*
- **Enterprise Users:** Solace is trusted by over 500 customers in mission critical IoT scenarios, including well-known brands.
- **Cluster Deployments:** Solace has over 60,000 cluster deployments globally.
- **GitHub Stars:** Solace has received over 13,000 stars on GitHub, indicating strong community support and adoption.
- **Downloads:** Solace has been downloaded over 40 million times.
- *f) Scalability*
- **Scalability:** Solace supports up to 100 million concurrent IoT device connections per cluster while maintaining 1 million messages per second throughput and sub-millisecond latency.
- **Cluster Size:** Solace can scale horizontally with a masterless distributed architecture, ensuring high availability and fault tolerance.
- **Benchmark:** Solace has demonstrated the capability to handle 200 million concurrent connections in a large-scale test scenario.
- *g) Industry Adoption*
- **Financial Services:** Solace is extensively used in the financial sector for secure and reliable messaging.
- **Healthcare:** Used by top healthcare companies for data integration and messaging.
- **E-commerce:** Companies like SAP and Verifone use Solace for order processing, tracking, and fulfillment.
- **Telecommunications:** Employed by major telecom companies for data integration and real-time processing.
- **Manufacturing:** Used by large manufacturing companies for data streaming and analytics.
- **Energy & Utilities:** Solace integrates with energy management and SCADA systems for smart grid management.

- **Automotive:** Solace is used by over 50 automotive companies, connecting more than 10 million electric and traditional vehicles.
- **Logistics:** A large transportation company uses Solace to handle 743.5 million customer tracking requests per day, saving 100 million miles and 10 million gallons of fuel per year.
- h) *Competitive Landscape*
- **Solace vs. Apache Kafka:** Kafka holds a larger market share and is preferred for high-throughput, low-latency applications, while Solace is often used for traditional messaging systems with strong transactional support.
- **Solace vs. RabbitMQ:** RabbitMQ has a higher market share and is favored for microservices architectures, whereas Solace is chosen for its reliability and exactly once message delivery.
- **Solace vs. IBM MQ:** IBM MQ is competitor with a larger market share, used for enterprise-grade messaging needs compared to Solace's cloud-native capabilities.

## 11) AWS IoT

AWS IoT is a robust and widely adopted IoT platform with a significant market share in the IoT platform market. It is used by thousands of companies globally, including major corporations like Siemens, Intel, and Volkswagen. AWS IoT's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in manufacturing, healthcare, automotive, energy, and smart cities. The competitive landscape includes other major players like Google Cloud IoT, Microsoft Azure IoT, and Cisco IoT, but AWS IoT's extensive feature set and proven performance give it a strong position in the market.

### a) Market Share & Geographical Distribution

- AWS IoT holds a significant market share in the IoT platform market. It is recognized as a leader in the 2024 Gartner Magic Quadrant for Global Industrial IoT Platforms.
- **Global Presence:** AWS IoT has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
- **United States:** 52.12% of AWS IoT's customers are based in the United States.
- **India:** 13.26% customers are based in India.
- **United Kingdom:** 8.84% of AWS IoT's customers are based in the United Kingdom.

### b) Growth Drivers

- **Cloud Ecosystem:** AWS IoT's integration with the broader AWS ecosystem provides a comprehensive solution for IoT applications, driving its adoption.
- **Scalability and Reliability:** AWS IoT's ability to scale and provide reliable messaging services ensures its popularity among enterprises

### c) Number of Users

- **Total Companies:** Over 718 companies have started using AWS IoT Core as an IoT platform tool globally.
- **Connected Devices:** AWS IoT connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

### d) Notable Corporate Users

- **Genpact, Ltd:** Uses AWS IoT for various IoT solutions.
- **Siemens AG:** Implements AWS IoT in its systems.
- **Intel Corporation:** Utilizes AWS IoT for secure and reliable messaging.
- **Birlasoft:** Employs AWS IoT for its IoT infrastructure.
- **Broadcom, Inc.:** Uses AWS IoT for its IoT solutions.
- **Volkswagen Group, Carrier, TC Energy, Bosch, BP, GE, Toyota, Invista, John Deere:** These global brands rely on AWS IoT for their industrial IoT applications.

### e) Customer Distribution by Company Size

- **20-49 Employees:** 128 companies.
- **100-249 Employees:** 103 companies.
- **10,000+ Employees:** 114 companies.

### f) Scalability

- **Scalability:** AWS IoT supports up to millions of concurrent IoT device connections, ensuring high availability and fault tolerance.
- **High Throughput:** AWS IoT can handle large volumes of data, making it suitable for high-load environments.
- **Global Reach:** AWS IoT Core is available in multiple AWS regions, including US East (N. Virginia), US West (Oregon), Europe (Frankfurt), Europe (Ireland), Asia Pacific (Sydney), Asia Pacific (Tokyo), and South America (São Paulo).

### g) Industry Adoption

- **Manufacturing:** AWS IoT is extensively used in the manufacturing sector for real-time data acquisition and smart factory solutions.
- **Healthcare:** Used by top healthcare companies for data integration and messaging.
- **Automotive:** Companies like Volkswagen and Toyota use AWS IoT for connected vehicle applications.
- **Energy & Utilities:** AWS IoT integrates with energy management and SCADA systems for smart grid management.
- **Smart Cities:** AWS IoT is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.

### h) Competitive Landscape

- **AWS IoT vs. Google Cloud IoT:** Google Cloud IoT holds an 18.85% market share and is a major competitor to AWS IoT.

- **AWS IoT vs. Microsoft Azure IoT:** Microsoft Azure IoT holds a 14.81% market share and is another significant competitor.
- **AWS IoT vs. Cisco IoT:** Cisco IoT holds a 10.48% market share, competing closely with AWS IoT in the IoT platform market.

## 12) Azure IoT

Azure IoT is a robust and widely adopted IoT platform with a significant market share in the IoT platform market. It is used by thousands of companies globally, including major corporations like Walmart, Robert Bosch GmbH, and Daimler Trucks North America. Azure IoT's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in manufacturing, healthcare, automotive, energy, and smart cities. The competitive landscape includes other major players like Google Cloud IoT, Cisco IoT, and Samsara, but Azure IoT's extensive feature set and proven performance give it a strong position in the market.

### a) Market Share & Geographical Distribution

- Microsoft Azure IoT holds a significant market share in the IoT platform market. It is recognized as a leader in the 2024 Gartner Magic Quadrant for Global Industrial IoT Platforms.
- **Global Presence:** Azure IoT has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
- **United States:** 47.72% of Azure IoT's customers are based in the United States.
- **India:** 14.04% of Azure IoT's customers are based in India.
- **United Kingdom:** 8.73% of Azure IoT's customers are based in the United Kingdom.

### b) Growth Drivers

- **Integration with Azure Services:** Azure IoT's seamless integration with other Azure services enhances its utility and drives its adoption in IoT applications.
- **Security and Compliance:** Robust security features and compliance with industry standards make Azure IoT a trusted solution for IoT deployments.

### c) Number of Users

- **Total Companies:** Over 1,396 companies have started using Microsoft Azure IoT as an IoT platform tool globally.
- **Connected Devices:** Azure IoT connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

### d) Notable Corporate Users

- **Walmart, Inc.:** Uses Azure IoT for various IoT solutions.
- **Robert Bosch GmbH:** Implements Azure IoT in its systems.
- **Daimler Trucks North America:** Utilizes Azure IoT for secure and reliable messaging.

- **Tetra Pak:** Employs Azure IoT for its IoT infrastructure.
- **Ernst & Young:** Uses Azure IoT for its IoT solutions.
- **Walgreens:** Implements Azure IoT in its systems.
- **Chevron:** Uses Azure IoT for industrial transformation and AI applications.
- **Electrolux Group:** Leverages Azure IoT for quality management in manufacturing processes.
- e) *Customer Distribution by Company Size*
  - **10,000+ Employees:** 244 companies.
  - **20-49 Employees:** 229 companies.
  - **1,000-4,999 Employees:** 211 companies.
- f) *Scalability*
  - **Scalability:** Azure IoT supports up to millions of concurrent IoT device connections, ensuring high availability and fault tolerance.
- **High Throughput:** Azure IoT can handle large volumes of data, making it suitable for high-load environments.
- **Global Reach:** Azure IoT Core is available in multiple Azure regions, including US East (N. Virginia), US West (Oregon), Europe (Frankfurt), Europe (Ireland), Asia Pacific (Sydney), Asia Pacific (Tokyo), and South America (São Paulo).

### g) Industry Adoption

- **Manufacturing:** Azure IoT is extensively used in the manufacturing sector for real-time data acquisition and smart factory solutions.
- **Healthcare:** Used by top healthcare companies for data integration and messaging.
- **Automotive:** Companies like Daimler Trucks North America and Volkswagen use Azure IoT for connected vehicle applications.
- **Energy & Utilities:** Azure IoT integrates with energy management and SCADA systems for smart grid management.
- **Smart Cities:** Azure IoT is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.

### h) Competitive Landscape

- **Azure IoT vs. Google Cloud IoT:** Google Cloud IoT holds a 19.59% market share and is a major competitor to Azure IoT.
- **Azure IoT vs. Cisco IoT:** Cisco IoT holds a 9.52% market share and is another significant competitor.
- **Azure IoT vs. Samsara:** Samsara holds a 9.30% market share, competing closely with Azure IoT in the IoT platform market.

## 13) Google IoT

Google Cloud IoT is a robust and widely adopted IoT platform with a significant market share in the IoT platform

market. It is used by thousands of companies globally, including major corporations like Chamberlain Group, Nutanix, and Hitachi. Google Cloud IoT's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in manufacturing, healthcare, automotive, energy, and smart cities. The competitive landscape includes other major players like Microsoft Azure IoT, Samsara, and Cisco IoT, but Google Cloud IoT's extensive feature set and proven performance give it a strong position in the market.

*a) Market Share & Geographical Distribution*

- Google Cloud IoT holds a market share of approximately 18.65% in the IoT platform category.
- **Global Presence:** Google Cloud IoT has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
- **United States:** 48.77% of Google Cloud IoT's customers are based in the United States.
- **India:** 16.58% of Google Cloud IoT's customers are based in India.
- **Germany:** 6.39% of Google Cloud IoT's customers are based in Germany.

*b) Growth Drivers*

- **Data Analytics Integration:** Google Cloud IoT's integration with Google Cloud's data analytics and machine learning services drives its adoption for advanced IoT applications.
- **Scalability and Performance:** The ability to handle large-scale IoT deployments with high performance and reliability is a significant growth driver

*c) Number of Users*

- **Total Companies:** Google Cloud IoT is used by over 1,790 companies globally.
- **Connected Devices:** Google Cloud IoT connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

*d) Notable Corporate Users*

- **Chamberlain Group:** Uses for various IoT solutions.
- **Nutanix, Inc.:** Implements in its systems.
- **Hitachi Ltd:** Utilizes Google Cloud IoT for secure and reliable messaging.
- **Apelon:** Employs Google IoT for its IoT infrastructure.
- **Philips:** Uses Google Cloud IoT for its IoT solutions.
- **Spotify, Snapchat, Best Buy:** These companies rely on Google Cloud IoT for their IoT applications.

*e) Customer Distribution by Company Size*

- **20-49 Employees:** 332 companies.
- **10,000+ Employees:** 293 companies.
- **100-249 Employees:** 233 companies.

*f) Scalability*

- **Scalability:** Google Cloud IoT supports up to millions of concurrent IoT device connections, ensuring high availability and fault tolerance.
- **High Throughput:** Google Cloud IoT can handle large volumes of data, making it suitable for high-load environments.
- **Global Reach:** Google Cloud IoT Core is available in multiple Google Cloud regions, ensuring global scalability and reliability.

*g) Industry Adoption*

- **Manufacturing:** Google Cloud IoT is extensively used in the manufacturing sector for real-time data acquisition and smart factory solutions.
- **Healthcare:** Used by top healthcare companies for data integration and messaging.
- **Automotive:** Companies like Hitachi and Philips use Google Cloud IoT for connected vehicle applications.
- **Energy & Utilities:** Google Cloud IoT integrates with energy management and SCADA systems for smart grid management.
- **Smart Cities:** Google Cloud IoT is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.

*h) Competitive Landscape*

- **Google Cloud IoT vs. Microsoft Azure IoT:** Microsoft Azure IoT holds a 14.90% market share and is a major competitor to Google Cloud IoT.
- **Google Cloud IoT vs. Samsara:** Samsara holds a 9.34% market share and is another significant competitor.
- **Google Cloud IoT vs. Cisco IoT:** Cisco IoT holds a 9.12% market share, competing closely with Google Cloud IoT in the IoT platform market.

*14) Amazon Kinesis*

Amazon Kinesis is a robust and widely adopted stream-processing platform with a significant market share in the IoT data streaming and analytics market. It is used by hundreds of companies globally, including major corporations like CommScope, Express Scripts, and Uber. Amazon Kinesis's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in manufacturing, healthcare, automotive, energy, and smart cities. The competitive landscape includes other major players like Apache Kafka, Apache Flink, and Apache Spark Streaming, but Amazon Kinesis's extensive feature set and proven performance give it a strong position in the market.

*a) Market Share and Geographical Distribution*

Amazon Kinesis holds a significant market share in the stream-processing market, with approximately 1.20%. It is a key player in the IoT data streaming and analytics space, providing robust solutions for real-time data processing.

- **Global Presence:** Amazon Kinesis has a strong global presence, with significant deployments across North America, Europe, and Asia-Pacific.

- **United States:** 61.78% of Amazon Kinesis's customers are based in the United States.
- **India:** 10.47% of Amazon Kinesis's customers are based in India.
- **United Kingdom:** 8.38% of Amazon Kinesis's customers are based in the United Kingdom.

*b) Growth Drivers*

- **Scalability and Performance:** Kinesis' ability to handle large volumes of data streams with high throughput and low latency is a significant growth driver, enabling real-time data processing and analytics for IoT applications.
- **Integration with AWS Ecosystem:** Kinesis' seamless integration with other AWS services, such as AWS IoT Core, AWS Lambda, and Amazon S3, simplifies IoT application development and deployment, driving adoption within the AWS ecosystem.
- **Managed Service:** As a fully managed service, Kinesis eliminates the need for infrastructure management, reducing operational overhead and enabling organizations to focus on their core IoT applications.

*c) Number of Users*

- **Total Companies:** Over 216 companies have started using Amazon Kinesis Data Streams (KDS) as a stream-processing tool globally.
- **Connected Devices:** Amazon Kinesis connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

*d) Notable Corporate Users*

- **CommScope Holding Company, Inc.:** Uses Amazon Kinesis for real-time data streaming and analytics.
- **Express Scripts:** Implements Amazon Kinesis in its systems for secure and reliable messaging.
- **Uber Technologies, Inc.:** Utilizes Amazon Kinesis for its IoT infrastructure and data processing needs.
- **Collins Aerospace:** Employs Amazon Kinesis for real-time data analytics and monitoring.
- **MTData:** Uses Amazon Kinesis for vehicle telematics and driver monitoring solutions.

*e) Customer Distribution by Company Size*

- 10,000+ Employees: 60 companies.
- 100-249 Employees: 30 companies.
- 20-49 Employees: 26 companies.

*f) User Statistics*

- **Revenue Distribution:** The majority of Amazon Kinesis customers fall into the large enterprise category, with significant usage among companies with over 10,000 employees.
- **Geographical Distribution:** Amazon Kinesis has a strong presence in the United States, India, and the United Kingdom, with a substantial number of users in these regions.

*g) Scalability*

- **Scalability:** Amazon Kinesis supports millions of concurrent device connections, ensuring high availability and fault tolerance.
- **High Throughput:** Amazon Kinesis can handle large volumes of data, making it suitable for high-load environments.
- **Global Reach:** Amazon Kinesis operates a globally distributed network, ensuring low latency and high availability for users worldwide.

*h) Industry Adoption*

- **Manufacturing:** Amazon Kinesis is extensively used in the manufacturing sector for real-time data acquisition and smart factory solutions.
- **Healthcare:** Used by top healthcare companies for data integration and real-time messaging.
- **Automotive:** Companies like Uber and Collins Aerospace use Amazon Kinesis for connected vehicle applications and industrial automation.
- **Energy & Utilities:** Amazon Kinesis integrates with energy management and SCADA systems for smart grid management.
- **Smart Cities:** Amazon Kinesis is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.

*i) Competitive Landscape*

- **Amazon Kinesis vs. Apache Kafka:** Apache Kafka holds a larger market share and is preferred for high-throughput, low-latency applications, while Amazon Kinesis is often used for its fully managed service and ease of integration with other AWS services.
- **Amazon Kinesis vs. Apache Flink:** Apache Flink is another significant competitor, offering robust stream processing capabilities, but Amazon Kinesis's integration with AWS services provides a competitive edge.
- **Amazon Kinesis vs. Apache Spark Streaming:** Apache Spark Streaming is a major player in the stream-processing market, but Amazon Kinesis's fully managed service and scalability make it a strong contender.

*15) Cisco IoT*

Cisco IoT is used by thousands of companies globally, including major corporations like Infosys, Wipro, and General Motors. Cisco IoT's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in manufacturing, healthcare, automotive, energy, and smart cities. The competitive landscape includes other major players like Microsoft Azure IoT, AWS IoT, and Google Cloud IoT, but Cisco IoT's extensive feature set and proven performance give it a strong position in the market.

*a) Market Share and Geographical Distribution*

- Cisco IoT holds a significant market share, being one of the top players globally for its comprehensive IoT

solutions that span various industries, including manufacturing, healthcare, and smart cities.

- **Global Presence:** Cisco IoT has a robust global presence, with significant deployments across North America, Europe, and Asia-Pacific.
- **United States:** A substantial portion of Cisco IoT's customers are based in the United States, reflecting its widespread adoption in the region.
- **Europe and Asia:** Cisco also has a strong user base in Europe and Asia, supporting a diverse range of applications and industries.

*b) Growth Drivers*

- **Edge Computing Capabilities:** Cisco's focus on edge computing and fog computing architectures is a significant growth driver, enabling real-time data processing and low-latency applications in IoT environments.
- **5G Readiness:** Cisco's IoT platforms, such as IoT Control Center, are 5G-ready, positioning the company to capitalize on the growth of 5G and the increasing demand for high-speed, low-latency connectivity in IoT deployments.
- **Connected Vehicles:** Cisco's dominance in the connected car market, with over 4 million devices added monthly to its IoT Control Center platform, drives growth as the automotive industry continues to embrace IoT technologies.

*c) Number of Users*

- **Total Companies:** Cisco IoT is used by over 129 companies globally, with a significant number of enterprise users.
- **Connected Devices:** Cisco IoT connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

*d) Notable Corporate Users*

- **Infosys Ltd:** Uses Cisco IoT for various IoT solutions.
- **Cisco Systems, Inc.:** Implements in its systems.
- **Wipro Ltd:** Utilizes Cisco IoT for secure and reliable messaging.
- **AT&T Inc:** Employs for its IoT infrastructure.
- **Cognizant Technology Solutions Corp:** Uses Cisco IoT for its IoT solutions.
- **General Motors:** Uses Cisco IoT to reimagine the experience of car ownership.
- **Vivint:** Uses Cisco IoT for home security systems.
- **ABB Robotics:** Uses to monitor robot connectivity and help customers service them proactively.

*e) Customer Distribution by Company Size*

- **Large Enterprises:** 49% of Cisco IoT customers are large enterprises with more than 1,000 employees.
- **Medium-Sized Companies:** 29% of Cisco IoT customers are medium-sized companies.
- **Small Companies:** 16% of Cisco IoT customers are small companies with fewer than 50 employees.

*f) User Statistics*

- **Revenue Distribution:** 47% of Cisco IoT customers have revenues greater than \$1 billion, 17% have revenues between \$50 million and \$1 billion, and 25% have revenues less than \$50 million.

- **Geographical Distribution:** 50% of Cisco IoT customers are in the United States, and 9% are in India.

*g) Scalability*

- **Scalability:** Cisco IoT supports millions of concurrent device connections, ensuring high availability and fault tolerance.

- **High Throughput:** Cisco IoT can handle large volumes of data, making it suitable for high-load environments.

- **Global Reach:** Cisco IoT operates a globally distributed network, ensuring low latency and high availability for users worldwide.

*h) Industry Adoption*

- **Manufacturing:** Cisco IoT is extensively used in the manufacturing sector for real-time data acquisition and smart factory solutions.

- **Healthcare:** Used by top healthcare companies for data integration and real-time messaging.

- **Automotive:** Companies like General Motors and ABB Robotics use Cisco IoT for connected vehicle applications and industrial automation.

- **Energy & Utilities:** Cisco IoT integrates with energy management and SCADA systems for smart grid management.

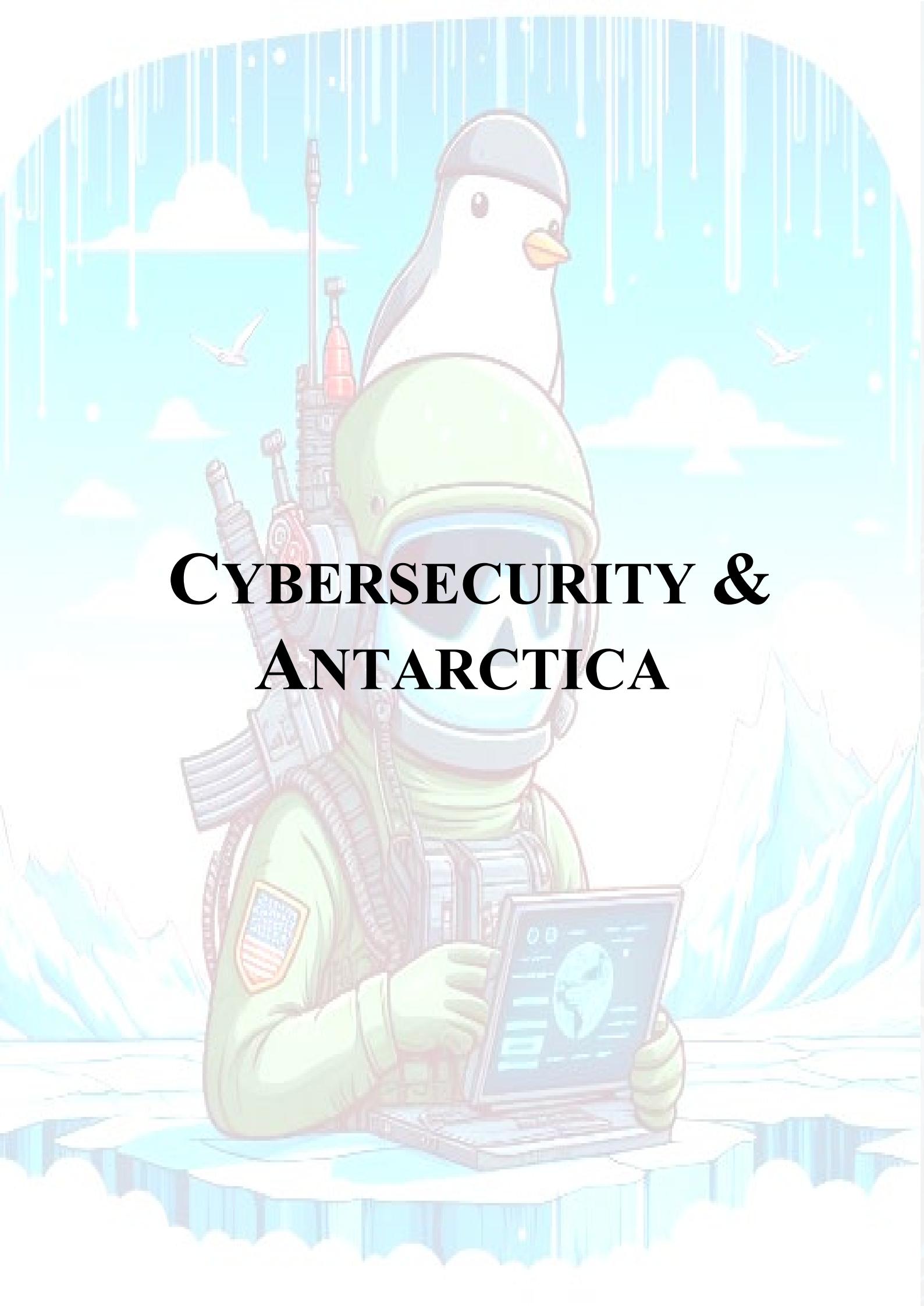
- **Smart Cities:** Cisco IoT is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.

*i) Competitive Landscape*

- **Cisco IoT vs. Microsoft Azure IoT:** Microsoft Azure IoT holds a significant market share and is a major competitor to Cisco IoT.

- **Cisco IoT vs. AWS IoT:** AWS IoT is another significant competitor, offering a comprehensive set of IoT services.

- **Cisco IoT vs. Google Cloud IoT:** Google Cloud IoT also competes closely with Cisco IoT in the IoT platform market.



# CYBERSECURITY & ANTARCTICA



*Abstract – quietly and unnoticed by the global community, especially the part that drives fundamental science forward, the United States has suspended its scientific research in the incredibly significant region of Antarctica. Yes, both on the colossal and almost unexplored continent and in the surrounding marine waters. The reason? It can be guessed in one try, as it has become common for the entire world: lack of funds. On other side, there is a strong need to manage specific cyber threats in Antarctica.*

#### A. Introduction

In April, the U.S. National Science Foundation (NSF) announced that it would not support any new field research this season due to delays in upgrading the McMurdo Station. The NSF and the U.S. Coast Guard also announced cuts that will jeopardize the U.S.'s scientific and geopolitical interests in the region for decades to come. Specifically, in April, the NSF announced that it would not renew the lease of one of its two Antarctic research vessels, the Laurence M. Gould. Prior to this, in October 2023, the NSF announced that it would operate only one research vessel in the coming decades.

Additionally, in March, the U.S. Coast Guard announced that it needed to "reassess baseline metrics" for its long-delayed Polar Security Cutter program, a vital program for U.S. national interests at both poles. Decisions made today will have serious consequences for U.S. activities in Antarctica well beyond 2050.

The State Department has refrained from announcing U.S. foreign policy interests in the Antarctic region, and the White House appears satisfied with an outdated and inconsistent national strategy for Antarctica from the last century. The U.S. Congress has also not responded to scientists' calls.

As a result, on April 1, the NSF's Office of Polar Programs announced that it is putting new fieldwork proposals on hold for the next two seasons and will not be soliciting new fieldwork proposals in Antarctica.

Ships capable of operating in polar seas are becoming increasingly in demand and difficult to build. Facing significant

challenges in the ice-class ship and vessel project, the U.S. Coast Guard announced in March that it would "shift baseline timelines" for developing new icebreaker projects.

The outcome of these seemingly independent decisions will be a reduction in the U.S. physical presence in Antarctica. This will have negative consequences not only for American scientists but also for U.S. geopolitics in the region, especially considering Russia's total superiority in icebreaker vessels and China's catching up.

The U.S. has missed the most important aspects: adequate and regular funding for Antarctic scientific research, a new national strategy for Antarctica (the current strategy was published in June 1994), and lawmakers' understanding of the importance of U.S. interests and decisions in Antarctica. The inability to fund the operational and logistical support necessary for U.S. scientific research and geopolitical influence effectively means the dominance of Russia and China in the Antarctic region, as no other country, including traditional Antarctic stakeholders like Chile, Australia, and Sweden, can surpass the existing and growing scientific potential of Russia and China.

#### 1) Keypoints

- **U.S. Reduces Antarctic Research Operations:** The U.S. has announced significant cutbacks in its Antarctic research operations due to funding issues and delays in upgrading critical infrastructure like the McMurdo Station. This includes not renewing the lease for the research vessel Laurence M. Gould and operating only one research vessel in the coming decades.
- **Challenges in U.S. Icebreaker Program:** The U.S. Coast Guard has announced delays in its Polar Security Cutter program, which is crucial for maintaining U.S. presence and operations in polar regions. This program's reassessment indicates significant challenges and potential long-term impacts on U.S. capabilities in Antarctica.
- **Geopolitical Implications of U.S. Withdrawal:** The reduction in U.S. presence in Antarctica has broader geopolitical implications, particularly as Russia and China continue to expand their capabilities and influence in the region. The lack of a modern national strategy and adequate funding for Antarctic operations puts the U.S. at a disadvantage.
- **Impact on Scientific Research:** The suspension of new fieldwork proposals by the NSF will impact scientific research in Antarctica, delaying important studies and potentially leading to a loss of valuable data. This decision highlights the broader issue of funding and support for scientific endeavors in remote regions.

#### B. Impact

The U.S. decision to suspend scientific research in Antarctica has prompted various responses from other countries, particularly those with significant interests and operations in the region. This decision, driven by budgetary constraints and delays in upgrading critical infrastructure, has implications for the geopolitical landscape and scientific collaboration in Antarctica.

**1) Geopolitical Consequences**

*a) Reduced U.S. Influence:*

- The reduction in U.S. presence will likely embolden other countries to pursue their individual interests in Antarctica. This shift could undermine the collective governance established by the Antarctic Treaty System, which emphasizes non-militarization and peaceful scientific collaboration.
- The U.S. has traditionally played a leadership role in Antarctic research, contributing to significant global scientific discoveries. A diminished presence could weaken this leadership and allow other nations, particularly China and Russia, to fill the void.

*b) Increased Presence of Rival Powers:*

- **China:** China has been expanding its presence in Antarctica, and the U.S. retreat is likely to accelerate this trend. China recently opened its fifth research station in Antarctica and has been increasing its scientific and logistical capabilities in the region. The expansion of Chinese activities raises concerns about potential dual-use technologies that could serve both scientific and military purposes. China's growing influence in Antarctica could shift the balance of power and increase geopolitical tensions.
- **Russia:** Russia has also been increasing its activities in Antarctica, including the establishment of new research stations. Russia's advancements in icebreaker technology and its strategic positioning in the region are likely to be bolstered by the reduced U.S. presence. This could lead to a more dominant Russian role in Antarctic governance and scientific research, further challenging U.S. interests.

*c) Responses from Traditional Antarctic Stakeholders*

- **Australia:** Australia, a key player in Antarctic affairs, has expressed concerns about the U.S. decision. Australia has been actively involved in Antarctic research and governance and relies on international collaboration to advance its scientific and environmental objectives. The U.S. retreat may prompt Australia to increase its own investments in Antarctic research and strengthen partnerships with other countries to fill the void left by the U.S.
- **United Kingdom:** The United Kingdom has also been a significant contributor to Antarctic research. The U.K. may seek to enhance its scientific presence and collaboration with other nations to ensure continued progress in Antarctic research. The U.K. government has emphasized the importance of maintaining a strong international presence in Antarctica to address global environmental challenges and uphold the principles of the Antarctic Treaty System

*d) Strategic Vulnerabilities:*

- The U.S. decision to scale back its operations could expose strategic vulnerabilities, particularly as emerging technologies lower barriers for countries

seeking to increase their presence and benefit from the region's resources. This includes the potential for military applications, such as reconnaissance and satellite positioning

- The lack of a robust U.S. presence could lead to a strategic imbalance, with Russia and China potentially dominating the region. This could have long-term implications for global security and U.S. national interests.

**2) Scientific and Environmental Implications**

*a) Impact on Scientific Research:*

- The suspension of new fieldwork proposals by the NSF will delay important scientific studies, leading to gaps in knowledge that are critical for understanding global environmental changes. This includes research on climate change, sea level rise, and ocean circulation patterns.
- The reduction in U.S. scientific activities could hinder international scientific collaboration, as many countries rely on U.S. infrastructure and logistical support for their research in Antarctica
- Environmental concerns are also paramount. Antarctica is a critical region for studying climate change and its effects on global ecosystems. The suspension of U.S. scientific research could slow progress in understanding and mitigating these impacts. Other countries may need to increase their research efforts to compensate for the reduced U.S. contribution, ensuring that critical environmental data continues to be collected and analyzed

*b) Environmental Risks:*

A reduced U.S. presence could impact environmental monitoring and conservation efforts. The Antarctic region is crucial for studying climate change and its effects on global ecosystems. A decline in research activities could slow progress in these areas and reduce the effectiveness of environmental protection measures.

*c) National Security:*

The U.S. decision to reduce its presence in Antarctica could have national security implications, particularly if rival powers use the region for military purposes. The strategic location of Antarctica makes it a potential site for reconnaissance and other military activities, which could threaten global security

**C. Cyber attacks**

The maritime industry in Antarctica faces a range of cyber threats, including phishing, malware, unauthorized access, GPS spoofing, supply chain attacks, and attacks on operational technology. These threats are compounded by the region's harsh environmental conditions and the increasing reliance on digital systems. Addressing these challenges requires a comprehensive cybersecurity strategy that includes robust defenses, continuous monitoring, and effective incident response capabilities.

*a) Phishing and Spear-Phishing Attacks*

- **Description:** These attacks involve deceptive emails and messages designed to trick maritime staff into revealing sensitive information or downloading malware. Phishing attacks can lead to unauthorized access to the ship's systems and sensitive data.

- **Impact:** Phishing can compromise navigation systems, communication networks, and operational technologies, potentially leading to significant operational disruptions.

*b) Malware and Ransomware*

- **Description:** Malicious software can be used to disrupt the operations of onboard systems, steal sensitive data, or lock out legitimate users, often demanding a ransom to restore access.

- **Impact:** Malware and ransomware attacks can cripple critical systems, leading to operational delays and financial losses. These attacks are particularly concerning given the reliance on digital systems for navigation and communication in Antarctica.

*c) Unauthorized Access and Insider Threats*

- **Description:** Unauthorized access involves gaining access to systems without permission, often through exploiting vulnerabilities or using stolen credentials. Insider threats involve employees or contractors who intentionally or unintentionally compromise security.

- **Impact:** Unauthorized access and insider threats can lead to data breaches, system disruptions, and loss of sensitive information. These threats are challenging to detect and mitigate, especially in isolated environments like Antarctica.

*2) GPS Spoofing*

- **Description:** Attackers manipulate GPS signals to mislead maritime navigation systems about the vessel's location or route.

- **Impact:** GPS spoofing can lead to navigation errors, unauthorized detours, and potential accidents. This is particularly dangerous in the treacherous waters around Antarctica, where precise navigation is crucial.

*3) Supply Chain Attacks*

- **Description:** These attacks target the interconnected systems and networks of the maritime supply chain, including ports, logistics providers, and other third-party services.

- **Impact:** Supply chain attacks can disrupt the entire maritime operation, leading to delays, financial losses, and compromised security of cargo and personnel.

*4) Cyber Attacks on Operational Technology (OT)*

- **Description:** OT systems, which include industrial control systems (ICS) used for navigation, engine control, and cargo handling, are increasingly targeted by cyber attackers.

- **Impact:** Attacks on OT systems can disrupt critical operations, leading to safety hazards, operational delays,

and significant financial losses. The integration of IT and OT systems in the maritime industry has increased the attack surface, making these systems more vulnerable.

*D. Unique cybersecurity challenges*

The maritime industry in Antarctica faces unique cybersecurity challenges that stem from its remote and harsh environment, the integration of legacy and modern systems, regulatory ambiguities, and a shortage of skilled professionals. Addressing these challenges requires international cooperation, continuous investment in cybersecurity measures, and the development of robust incident response capabilities.

*1) Harsh Environmental Conditions*

- **Extreme Weather:** The severe and unpredictable weather conditions in Antarctica can disrupt communication and power systems, making it difficult to maintain consistent cybersecurity measures.
- **Isolation:** The remote and isolated nature of Antarctic operations means that physical access to infrastructure for maintenance and incident response is limited, complicating cybersecurity efforts.

*2) Integration of IT and OT Systems*

- **Complex Integration:** The maritime industry, including operations in Antarctica, increasingly relies on the integration of Information Technology (IT) and Operational Technology (OT) systems. This integration creates complex cybersecurity challenges as these systems were traditionally separate and are now interconnected, increasing the attack surface.
- **Legacy Systems:** Many maritime operations still use legacy systems that were not designed with cybersecurity in mind. These systems are now connected to modern networks, creating vulnerabilities that can be exploited by cyber attackers.

*3) Regulatory and Compliance Issues*

- **Regulatory Ambiguities:** The maritime industry faces regulatory ambiguities, especially in remote regions like Antarctica. Existing regulations, such as the International Ship and Port Facility Security (ISPS) Code and the Maritime Transportation Security Act (MTSA), were conceived in a pre-digital era and may not fully address current cyber threats.
- **International Cooperation:** Given the global nature of maritime operations, international cooperation is essential for establishing uniform cybersecurity standards and protocols. This is particularly challenging in Antarctica, where multiple countries have interests and operations.

*4) Technological Advancements and Threats*

- **Increased Connectivity:** The adoption of cloud computing, the Internet of Things (IoT), and autonomous technologies in maritime operations has led to increased interconnectivity between IT and OT systems. This connectivity heightens cybersecurity

risks, as evidenced by a 900% increase in cyberattacks on maritime OT systems over the past three years.

- **Emerging Threats:** The maritime industry is a prime target for cyber threats, including nation-state attackers and cybercriminals looking to disrupt operations, steal data, or demand ransoms. The evolving threat landscape requires continuous monitoring and updating of cybersecurity measures.
- 5) *Workforce and Expertise*
- **Shortage of Cybersecurity Professionals:** There is a pervasive shortage of skilled cybersecurity professionals in the maritime industry. This shortage is exacerbated in remote regions like Antarctica, where attracting and retaining talent is particularly challenging.
  - **Training and Awareness:** Continuous training and awareness programs are essential to maintain a high level of cybersecurity readiness. However, the logistical challenges of conducting such programs in Antarctica can hinder their effectiveness.

6) *Incident Response and Recovery*

- **Limited Incident Response Capabilities:** The ability to respond to and recover from cyber incidents is limited in Antarctica due to the region's isolation and harsh conditions. This makes it crucial to have robust remote monitoring and incident response capabilities.
- **Cyber Incident Reporting:** The recent Executive Order by the Biden-Harris Administration emphasizes the need for cyber incident reporting. However, implementing these requirements in Antarctica can be challenging due to communication constraints and regulatory differences.

*E. Cybersecurity Measures for the specific cases*

The maritime industry in Antarctica can effectively address cybersecurity threats by adopting a holistic cybersecurity framework, adhering to regulatory standards, leveraging advanced technological solutions, providing comprehensive training, developing robust incident response plans, and fostering international cooperation. These measures are essential for safeguarding maritime operations in one of the most challenging and remote regions of the world.

1) *Holistic Cybersecurity Framework*

- **Integration of IT and OT Security:** The convergence of Information Technology (IT) and Operational Technology (OT) systems in the maritime industry necessitates a holistic approach to cybersecurity. Utilizing frameworks like the NIST Cybersecurity Framework and the ISA/IEC IACS Cybersecurity Lifecycle model helps in assessing, planning, implementing, and monitoring cybersecurity measures across both IT and OT environments.
- **Comprehensive Risk Management:** Developing and implementing a wide range of enterprise cybersecurity controls that span both onboard vessels and shoreside facilities is essential. This includes addressing IT, OT,

and IoT systems to ensure a secure maritime critical infrastructure.

2) *Regulatory Compliance and Standards*

- **Adherence to IMO Guidelines:** The International Maritime Organization (IMO) has issued guidelines on maritime cyber risk management, which provide high-level recommendations and functional elements to minimize risks and impact on shipping-related operations, safety, and security.
- **Compliance with ATS and UNCLOS:** The Antarctic Treaty System (ATS) and the United Nations Convention on the Law of the Sea (UNCLOS) provide a legal framework for maritime operations in Antarctica. Ensuring compliance with these regulations, including vessel registration and safety equipment requirements, is crucial for maintaining maritime security.

3) *Advanced Technological Solutions*

- **Network Segmentation:** Dividing the network into separate segments helps contain potential breaches and makes lateral movements harder for attackers. This is particularly important for protecting critical systems on vessels and in port facilities.
- **Regular Penetration Testing:** Conducting regular penetration tests to identify and address vulnerabilities before they can be exploited by attackers is a proactive measure to enhance cybersecurity.
- **AI and Machine Learning:** Implementing advanced threat detection systems that use artificial intelligence and machine learning to detect unusual behavior can help identify and mitigate cyber threats in real-time.
- **Advanced Cybersecurity Systems:** The use of advanced cybersecurity systems, such as Cydome's Everlight, supports vessel cybersecurity management through real-time monitoring and risk assessment. These systems help detect and mitigate cyber threats effectively

4) *Training and Awareness*

- **Cybersecurity Training Programs:** Providing comprehensive cybersecurity training to all personnel, both seafarers and shore-based staff, is essential. Training programs should cover the latest security risks, phishing tactics, and best practices for preventing cyber-attacks.
- **User Education and Awareness:** Regularly updating employees on cybersecurity best practices and the latest threats ensures that they are better prepared to detect and prevent cyber-attacks, reducing the risk of human error.

5) *Incident Response and Recovery*

- **Incident Response Plan:** Developing and regularly updating an incident response plan ensures quick action and mitigation if a breach occurs. This plan should include clear protocols for detecting, responding to, and recovering from cyber incidents.
- **Remote Monitoring and Management:** Given the isolation and harsh conditions of Antarctica, robust remote monitoring and management tools are essential

for maintaining cybersecurity measures and responding to incidents effectively.

#### 6) International Cooperation and Collaboration

- Global Standards and Protocols:** International cooperation is vital for establishing uniform cybersecurity standards and protocols that transcend national boundaries. Collaboration between government agencies, industry stakeholders, and international partners helps enhance cybersecurity standards and share best practices.
- Cyber Incident Reporting:** Implementing mandatory cyber incident reporting, as emphasized by recent executive orders, helps in timely detection and response to cyber threats. This is crucial for maintaining the security of maritime operations in remote regions like Antarctica.

#### F. Companies' training

Maritime companies in Antarctica are addressing cybersecurity threats by implementing comprehensive and continuous training programs for their employees. These programs are aligned with international standards, use advanced training tools, and focus on reducing human error. By ensuring that employees are well-trained in identifying and avoiding cyber threats, these companies can better protect their operations in the challenging and remote environment of Antarctica.

##### 1) Comprehensive Cybersecurity Training Programs

- Cyber Security Awareness Courses:** Companies are providing online courses specifically designed for ship crew members. These courses cover extensive knowledge about maritime cybersecurity, including the types of information vulnerable to cyber-attacks, stages of a cyber-attack, and mitigation measures.
- Holistic Training Approaches:** Training programs are designed to cover a wide range of topics, including the latest security risks, policies, and procedures. This helps in reducing human error, which is one of the top causes of cybersecurity incidents on ships.

##### 2) Regular and Updated Training Sessions

- Continuous Education:** Regularly updating training programs to include the latest cybersecurity threats and best practices ensures that employees remain vigilant and informed. This includes training on the latest phishing tactics and other common cyber threats.
- Incident Response Training:** Employees are trained on how to respond appropriately to cybersecurity incidents, which helps in minimizing damage and ensuring critical operations continue running smoothly.

##### 3) Compliance with International Standards

- IMO Guidelines:** Training programs are aligned with the International Maritime Organization (IMO) guidelines on maritime cyber risk management. These guidelines provide high-level recommendations and functional elements to minimize risks and impact on shipping-related operations, safety, and security.

- STCW Convention:** The International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW) is being reviewed to include 'cybersecurity awareness' as a standalone area of developing competencies. This ensures that seafarers are trained in digital skills, communications, information management, and the ability to adapt to a changing work environment.

##### 4) Use of Advanced Training Tools

- Simulators and Practical Exercises:** The use of simulators and practical exercises in training programs helps employees understand and manage real-world cyber threats. This hands-on approach is crucial for developing practical skills in identifying and mitigating cyber threats.
- AI and Machine Learning:** Advanced threat detection systems that use artificial intelligence and machine learning are being integrated into training programs. These systems help employees learn how to detect unusual behavior that may indicate a cyber threat.

##### 5) Focus on Reducing Human Error

- Awareness Campaigns:** Regular awareness campaigns and training sessions help in reducing human error by increasing awareness of security risks, policies, and procedures.
- Phishing Simulations:** Conducting phishing simulations as part of the training helps employees recognize and avoid phishing attempts, which are a common method to gain unauthorized access to systems.

#### G. Regulations for the maritime industry in antarctica

The latest cybersecurity regulations for the maritime industry in Antarctica are shaped by a combination of international frameworks like the Antarctic Treaty System (ATS) and the United Nations Convention on the Law of the Sea (UNCLOS), as well as specific guidelines from the International Maritime Organization (IMO). Additionally, recent U.S. Executive Orders have introduced new cybersecurity requirements and standards, emphasizing the need for comprehensive cyber risk management and incident reporting. International cooperation and collaboration remain essential for establishing and maintaining effective cybersecurity measures in the maritime industry.

##### 1) Antarctic Treaty System (ATS)

- Overview:** The ATS is an international framework of agreements that govern activities in Antarctica. It includes provisions for the peaceful use of the continent, environmental protection, and the facilitation of scientific research.
- Maritime Security:** The ATS requires all vessels entering and leaving Antarctic territorial waters to be registered with the Antarctic Treaty Secretariat. It also mandates the enforcement of safety regulations and the monitoring of vessels to ensure compliance with international navigation rules.

2) *United Nations Convention on the Law of the Sea (UNCLOS)*

- **Maritime Law:** UNCLOS provides a comprehensive set of rules governing the sea and its resources, including the right of countries to navigate the seas and the responsibility to protect and preserve the marine environment.
- **Cybersecurity Provisions:** While UNCLOS primarily addresses traditional maritime security issues, its principles are foundational for the development of cybersecurity measures in the maritime domain. It emphasizes the need for cooperation among states to ensure maritime security, which includes addressing cyber threats.

3) *International Maritime Organization (IMO) Guidelines*

- **Cyber Risk Management:** The IMO has introduced guidelines for managing cyber risks to ships and shipping, including a requirement for companies to develop cyber risk management plans. These guidelines provide high-level recommendations and functional elements to minimize risks and impact on shipping-related operations, safety, and security.
- **MSC-FAL.1-Circ.3-Rev.2:** This guideline on maritime cyber risk management, issued in July 2022, offers high-level recommendations and is highly dependent on the interpretation of the individual or company implementing it.

4) *U.S. Executive Orders and Federal Rules*

- **Biden Administration's Executive Order:** On February 21, 2024, President Biden signed an Executive Order aimed at improving the cybersecurity of U.S. ports and maritime supply chains. This order introduces new cybersecurity requirements and standards for stakeholders of the U.S. Marine Transportation System (MTS) and increases the authority of the U.S. Coast Guard to address cyber threats.
- **Cyber Incident Reporting:** The Executive Order mandates the reporting of actual or potential cyber incidents that could endanger harbors, ports, or waterfront facilities. This includes sharing reports with the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI).

5) *International Cooperation and Collaboration*

- **Global Standards and Protocols:** Given the global nature of maritime operations, international cooperation is essential for establishing uniform cybersecurity standards and protocols. Collaboration between government agencies, industry stakeholders, and international partners is crucial for enhancing cybersecurity standards and sharing best practices.
- **Regulatory Bodies:** Regulatory frameworks for maritime cybersecurity are still evolving, leading to inconsistencies and implementation challenges. The IMO and other international bodies continue to refine and update guidelines to address the growing cyber threats in the maritime industry.

H. *Economic consequences*

Cyberattacks on the maritime industry in Antarctica can have far-reaching economic impacts, including disruptions to scientific research and operations, increased operational costs, supply chain disruptions, loss of sensitive data and intellectual property, and heightened national security and geopolitical tensions.

- 1) *Disruption of Scientific Research and Operations*
  - **Impact on Research Missions:** Cyberattacks can disrupt the operations of research vessels and stations, leading to delays or cancellations of scientific missions. This can result in the loss of valuable research data and increased costs associated with rescheduling and extending missions.
  - **Operational Delays:** Disruptions to navigation systems, communication networks, and other critical operational technologies can lead to significant delays in maritime operations. This can increase operational costs and reduce the efficiency of research and supply missions.
- 2) *Increased Operational Costs*
  - **Mitigation and Recovery Costs:** The costs associated with mitigating and recovering from cyberattacks can be substantial. This includes expenses related to incident response, system restoration, and implementing additional cybersecurity measures to prevent future attacks.
  - **Insurance Premiums:** Cyberattacks can lead to higher insurance premiums for maritime companies operating in Antarctica. Insurers may increase premiums to cover the heightened risk of cyber incidents, adding to the overall operational costs.
- 3) *Supply Chain Disruptions*
  - **Impact on Logistics:** Cyberattacks can disrupt the supply chain by affecting the transportation of goods and essential supplies to and from Antarctica. This can lead to shortages of critical supplies, increased transportation costs, and delays in the delivery of goods.
  - **Economic Ripple Effects:** Disruptions in the supply chain can have ripple effects on the broader economy, affecting industries that rely on timely deliveries of goods and materials. This can lead to increased costs and reduced productivity across multiple sectors.
- 4) *Loss of Sensitive Data and Intellectual Property*
  - **Data Breaches:** Cyberattacks can result in the theft of sensitive data, including research findings, proprietary information, and personal data of crew members and researchers. The loss of such data can have significant economic implications, including the loss of competitive advantage and potential legal liabilities.
  - **Intellectual Property Theft:** The theft of intellectual property, such as proprietary research data and technological innovations, can undermine the economic value of scientific research and development efforts in Antarctica.

- 5) *Impact on National Security and Geopolitical Interests*
- **Geopolitical Tensions:** Cyberattacks on maritime operations in Antarctica can exacerbate geopolitical tensions, particularly if they are attributed to nation-state actors. This can lead to increased defense and security expenditures as countries seek to protect their interests in the region.
  - **Strategic Vulnerabilities:** The disruption of maritime operations can expose strategic vulnerabilities, potentially affecting national security and economic stability. This can lead to increased investments in cybersecurity and defense measures, diverting resources from other critical areas.

#### I. Non-economic consequences

The non-economic consequences of cyberattacks on the maritime industry in Antarctica are significant and multifaceted. They include threats to safety and human life, environmental damage, geopolitical tensions, disruption of scientific research, and operational challenges.

##### 1) Safety and Human Life

- **Crew Safety:** Cyberattacks can compromise the safety of crew members by disrupting critical systems such as navigation, communication, and engine controls. This can lead to accidents, groundings, or collisions, putting lives at risk.
- **Search and Rescue Operations:** Disruptions to communication and navigation systems can hinder search and rescue operations, making it difficult to locate and assist vessels in distress. This can result in delayed response times and increased risk to human life.

##### 2) Environmental Impact

- **Pollution and Spills:** Cyberattacks that disrupt navigation or engine control systems can lead to accidents that result in oil spills or the release of hazardous materials into the fragile Antarctic environment. Such incidents can have long-lasting detrimental effects on marine ecosystems and wildlife.
- **Ecosystem Damage:** The Antarctic region is home to unique and sensitive ecosystems. Cyber-induced accidents can cause significant damage to these ecosystems, affecting biodiversity and the overall health of the environment.

##### 3) Geopolitical and Security Implications

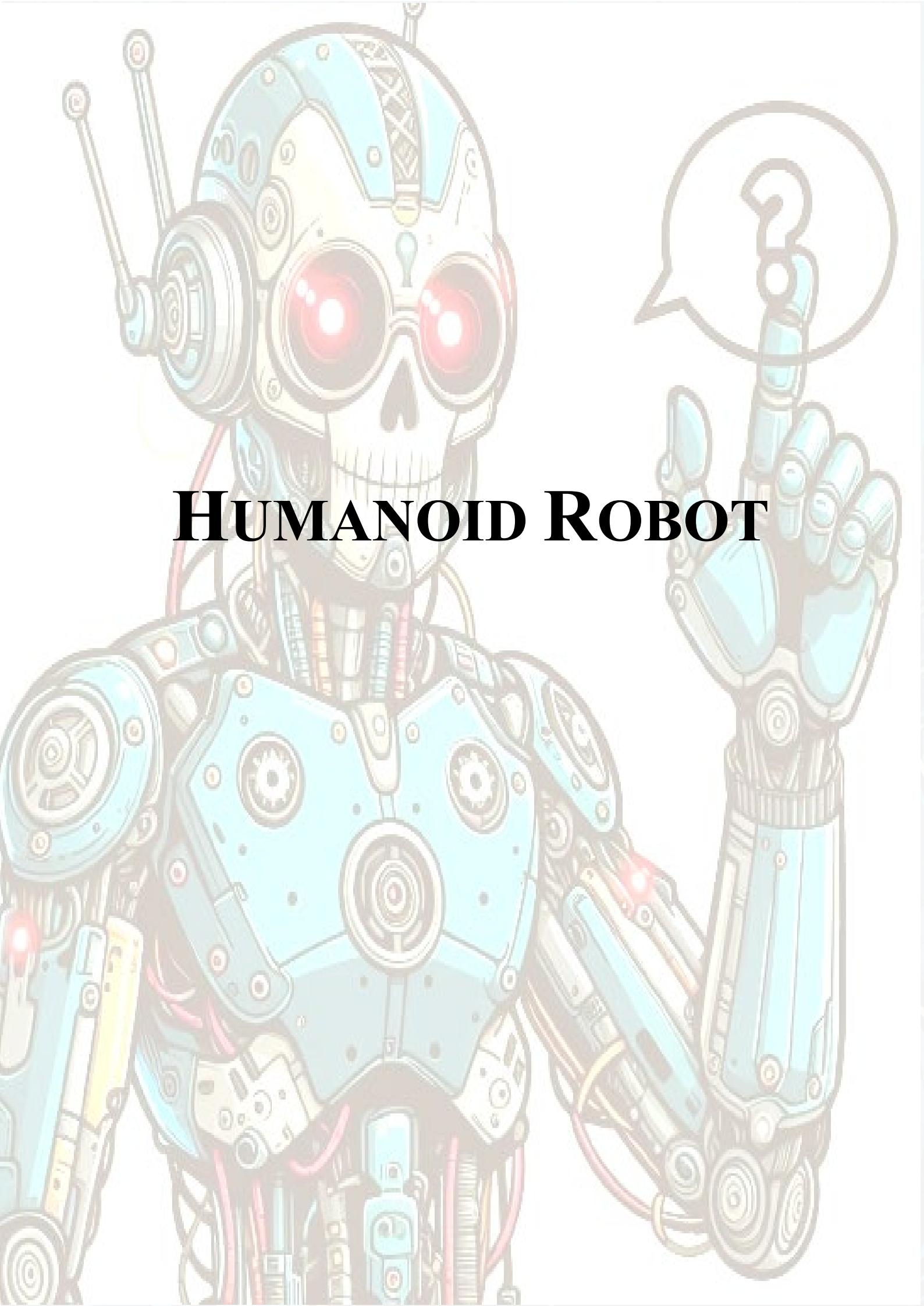
- **Geopolitical Tensions:** Cyberattacks on maritime operations in Antarctica can exacerbate geopolitical tensions, particularly if they are attributed to nation-state actors. This can lead to increased military presence and heightened security measures in the region, potentially escalating conflicts.
- **National Security:** The disruption of maritime operations can expose strategic vulnerabilities, affecting national security. This is particularly relevant for countries with significant interests in Antarctica, as cyberattacks can undermine their ability to protect and assert their claims and interests in the region.

##### 4) Disruption of Scientific Research

- **Impact on Research Missions:** Cyberattacks can disrupt the operations of research vessels and stations, leading to delays or cancellations of scientific missions. This can result in the loss of valuable research data and hinder scientific progress in understanding climate change, marine biology, and other critical areas.
- **Data Integrity:** Cyberattacks can compromise the integrity of scientific data, leading to inaccurate or incomplete research findings. This can undermine the credibility of scientific research and affect policy decisions based on such data.

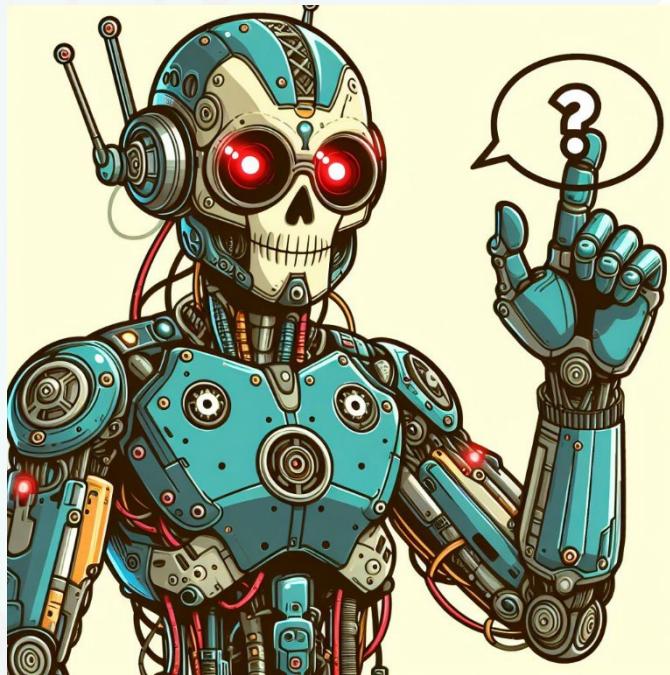
##### 5) Operational and Logistical Challenges

- **Operational Disruptions:** Cyberattacks can disrupt the day-to-day operations of maritime vessels, affecting everything from navigation to cargo handling. This can lead to significant logistical challenges, including delays in the delivery of essential supplies and equipment to research stations.
- **Communication Breakdown:** Disruptions to communication systems can isolate vessels and research stations, making it difficult to coordinate activities and respond to emergencies. This can increase the risk of accidents and hinder effective crisis management.



# HUMANOID ROBOT





*Abstract – this document provides a comprehensive analysis of the humanoid robot challenges, focusing on various critical aspects that are pivotal for security professionals and other industry specialists. The analysis delves into the technological advancements in humanoid robots, particularly the integration of end-to-end AI and multi-modal AI algorithms, which significantly enhance the robots' capabilities in handling complex tasks and decision-making processes. The document also examines the economic implications, emphasizing the potential of humanoid robots in substituting human roles, thereby not only increasing safety but also addressing labor shortages in critical sectors and strategic implications of these technological advancements on global labor markets and industrial competitiveness.*

*This document is beneficial for security professionals who are interested in understanding the implications of robotic automation on cybersecurity measures and infrastructure protection. Additionally, the analysis serves as a valuable resource for industry specialists across various sectors, providing insights into how humanoid robots can be integrated into their operations to enhance efficiency, safety, and innovation.*

#### A. Introduction

Humanoid robots are advanced machines designed to mimic human form and behavior, equipped with articulated limbs, advanced sensors, and often the ability to interact socially. These robots are increasingly being utilized across various sectors, including healthcare, education, industry, and services, due to their adaptability to human environments and their ability to perform tasks that require human-like dexterity and interaction.

In healthcare, humanoid robots assist with clinical tasks, provide emotional support, and aid in-patient rehabilitation. In education, they serve as interactive companions and personal tutors, enhancing learning experiences and promoting social integration for children with special needs. The industrial sector benefits from humanoid robots through automation of repetitive and hazardous tasks, improving efficiency and safety. Additionally, in service industries, these robots handle customer

assistance, guide visitors, and perform maintenance tasks, showcasing their versatility and potential to transform various aspects of daily life.

#### B. Market Forecasts for Humanoid Robots

The humanoid robot market is poised for substantial growth, with projections indicating a multi-billion-dollar market by 2035. Key drivers include advancements in AI, cost reductions, and increasing demand for automation in hazardous and manufacturing roles.

- **Goldman Sachs Report (January 2024):**
  - **Total Addressable Market (TAM):** The TAM for humanoid robots is expected to reach \$38 billion by 2035, up from an initial forecast of \$6 billion. This increase is driven by a fourfold rise in shipment estimates to 1.4 million units.
  - **Shipment Estimates:** The base case scenario predicts a 53% compound annual growth rate (CAGR) from 2025 to 2035, with shipments reaching 1.4 million units by 2035. The bull case scenario anticipates shipments hitting 1 million units by 2031, four years ahead of previous expectations.
  - **Cost Reductions:** The Bill of Materials (BOM) cost for high-spec robots has decreased by 40% to \$150,000 per unit in 2023, down from \$250,000 the previous year, due to cheaper components and a broader domestic supply chain.
- **Data Bridge Market Research:** The global humanoid robot market is expected to grow from \$2.46 billion in 2023 to \$55.80 billion by 2031, with a CAGR of 48.5% during the forecast period.
- **SkyQuestt:** The market is projected to grow from \$1.48 billion in 2019 to \$34.96 billion by 2031, with a CAGR of 42.1%.
- **GlobeNewswire:** The global market for humanoid robots, valued at approximately \$1.3 billion in 2022, is anticipated to expand to \$6.3 billion by 2030, with a CAGR of 22.3%.
- **The Business Research Company:** The market is expected to grow from \$2.44 billion in 2023 to \$3.7 billion in 2024, with a CAGR of 51.6%. By 2028, the market is projected to reach \$19.69 billion, with a CAGR of 51.9%.
- **Grand View Research:** Market Size: The global humanoid robot market was estimated at \$1.11 billion in 2022 and is expected to grow at a CAGR of 21.1% from 2023 to 2030.
- **Goldman Sachs (February 2024):** In a blue-sky scenario, the market could reach up to \$154 billion by 2035, comparable to the global electric vehicle market and one-third of the global smartphone market as of 2021.
- **Macquarie Research:** Under a neutral assumption, the global humanoid robot market is expected to reach \$107.1 billion by 2035, with a CAGR of 71% from 2025 to 2035.

**1) Key Drivers and Trends**

- **Technological Advancements:** Significant progress in AI, particularly in end-to-end AI and multi-modal AI algorithms, is accelerating product iterations and improving robot capabilities.
- **Cost Reductions:** The availability of cheaper components and improvements in design and manufacturing techniques are driving down costs, making humanoid robots more economically viable.
- **Labor Market Implications:** The demand for robots to handle hazardous and dangerous jobs is elevated by national policies, with potential applications in manufacturing, disaster rescue, and elderly care.
- **Investment and Market Dynamics:** Increased investments from supply chains, startups, and listed companies, particularly in the US and Asia, are driving market growth. Government support, especially from China, is also a significant factor.

**C. Technological Advancements**

The development of humanoid robots has seen significant technological advancements, driven by improvements in artificial intelligence (AI), machine learning, sensor integration, and hardware design. These advancements are enabling humanoid robots to perform increasingly complex tasks and interact more naturally with human environments.

**1) AI and Machine Learning Integration**

- **End-to-End AI:** The integration of end-to-end AI and multi-modal AI algorithms has been a game-changer, enabling faster product iterations and improved capabilities in humanoid robots. This approach allows robots to execute tasks from original commands to final outputs under AI self-generated rules, rather than pre-programmed rules by software engineers.
- **Reinforcement Learning (RL):** RL frameworks, such as the one used in the development of the humanoid robot "Adam," have significantly improved the efficiency and effectiveness of imitation learning processes. These frameworks enable robots to achieve human-comparable performance in complex locomotion tasks by using human locomotion data for imitation learning.
- **Large Language Models (LLMs):** The integration of multimodal LLMs, such as Google Gemini and ChatGPT 4 Multimodal, enhances the robots' ability to 'hear' and 'see,' facilitating more nuanced and interactive engagement with the world. This convergence is redefining human-robot interactions, enabling robots to operate seamlessly in real-world environments.

**2) Sensor Integration and Fusion**

- **Advanced Sensors:** Humanoid robots are equipped with a variety of sensors, including inertial measuring units (IMUs) for spatial awareness, LiDAR for depth sensing, and cameras for visual perception. These sensors allow robots to sense and comprehend their surroundings, enabling them to navigate, communicate, and make decisions autonomously.

- **Sensor Fusion Techniques:** Techniques such as neural networks, Bayesian inference, and Kalman filtering are used to combine sensor data in real-time, providing a comprehensive picture of the robot's environment. This allows robots to predict their posture, map their environment, and identify objects and obstacles in their path.

**3) Hardware and Design Improvements**

- **Cost Reductions:** The Bill of Materials (BOM) cost for high-spec robots has decreased significantly, driven by the availability of cheaper components and a broader domestic supply chain. This reduction in costs is accelerating the timeline for factory and consumer applications of humanoid robots.
- **Innovative Structural Designs:** New structural designs, such as those used in the "Adam" robot, improve the efficiency and effectiveness of the imitation learning process. These designs enable robots to exhibit unprecedented human-like characteristics in locomotion tasks.
- **Battery and Actuator Enhancements:** Improvements in battery life and actuator design are critical for enhancing the mobility and agility of humanoid robots. For instance, robots equipped with hydraulic actuators can typically work in short bursts, but advancements in battery technology are expected to enable longer operational periods.

**4) Human-Robot Interaction and Cognitive Abilities**

- **Cognitive Algorithms:** Researchers are developing algorithms that mimic important facets of human cognition, such as perception, attention, memory, learning, and reasoning. These cognitive abilities allow robots to decipher sensory input, concentrate on relevant inputs, store and retrieve knowledge, and plan actions based on predictions.
- **Emotional and Social Interaction:** Humanoid robots like PEPPEP are designed to provide emotional support by detecting facial expressions and vocal tones, adjusting their interactions to create a comforting environment. This capability is particularly valuable in healthcare settings.

**5) Real-World Applications and Use Cases**

- **Industrial and Hazardous Environments:** Humanoid robots are increasingly being used in industrial settings to automate repetitive and potentially dangerous tasks. Their agility and precision are leveraged in the inspection and maintenance of hostile environments, increasing the efficiency of industrial operations.
- **Healthcare and Education:** In healthcare, humanoid robots assist with clinical tasks and provide emotional support to patients. In education, they serve as interactive companions and personal tutors, promoting social integration and personalized learning experiences.

**D. Labor Market Implications of Humanoid Robots**

The integration of humanoid robots into various industries is expected to have profound implications for the labor market. These implications span job displacement, job creation, changes in job roles, and the need for workforce reskilling.

**1) Job Displacement and Creation**

- **Displacement of Routine Jobs:** Humanoid robots are likely to replace jobs that involve repetitive, manual, and routine tasks. This includes roles such as production-line workers, quality-control assessors, and machine operators. The deployment of robots in these areas can lead to significant job losses, particularly in manufacturing and automotive industries.
- **Creation of New Jobs:** While robots may displace certain jobs, they also create new opportunities, particularly in high-skilled roles. These new jobs include AI machine specialists, robot programmers, and maintenance technicians. The shift towards more advanced roles requires workers to develop new skills and adapt to working alongside robots.

**2) Impact on Wages and Employment**

- **Wage Decline:** The introduction of robots into the labor market has been associated with a decline in wages. For instance, studies have shown that for every robot added per 1,000 workers, wages decline by approximately 0.42%, and the employment-to-population ratio decreases by 0.2 percentage points.
- **Employment Reduction:** The deployment of robots can lead to a reduction in employment opportunities. Research indicates that one more robot per thousand workers reduces the employment-to-population ratio by between 0.18 and 0.34 percentage points.

**3) Sector-Specific Impacts**

- **Manufacturing:** The manufacturing sector is expected to see significant changes due to the integration of humanoid robots. Robots can handle tasks such as electric vehicle assembly, component sorting, and other structured environment jobs. This could fill 4% of the projected US manufacturing labor shortage by 2030.
- **Elderly Care:** Humanoid robots are also projected to address 2% of global elderly care demand by 2035. This application is particularly relevant in countries with aging populations and a shortage of caregivers.

**4) Workforce Reskilling and Adaptation**

- **Reskilling Initiatives:** To mitigate the negative impacts of job displacement, there is a need for comprehensive reskilling and upskilling programs. These programs should focus on equipping workers with the skills needed to operate and collaborate with robots. Governments and businesses must invest in education and training to prepare the workforce for the future.
- **Adaptation to New Roles:** Workers will need to adapt to new roles that involve more complex, creative, and empathetic tasks. Robots will take over monotonous and physically demanding tasks, allowing humans to focus on higher-value work.

**5) Economic and Social Implications**

- **Productivity and GDP Growth:** The adoption of robots is expected to lead to significant productivity gains, which in turn can boost gross domestic product (GDP). For example, the increasing use of industrial robots has been shown to raise the annual growth of GDP by 0.36% across 17 countries.

- **Economic Inequality:** The benefits of automation and robotics are likely to accrue to capital owners and skilled workers, potentially increasing economic inequality. It is crucial to implement policies that ensure equitable access to the benefits of automation and support for displaced workers.

**6) Ethical and Social Considerations**

- **Human-Robot Interaction:** The rise of humanoid robots raises ethical concerns about the replacement of human relations with robotic ones. From the perspective of ubuntu philosophy, human relations are essential for becoming fully human, and robotic relations may lead to social isolation and reduced moral agency.
- **Policy and Regulation:** There is a need for robust ethical frameworks and regulations to guide the deployment and use of humanoid robots. This includes considerations around privacy, security, and the ethical implications of robots taking on roles traditionally held by humans

**E. Increased Investments and Funding**

The sources highlight the significant investments and funding pouring into the humanoid robotics sector, driven by the potential of this emerging technology and the involvement of major tech companies and investors.

- **Figure AI's Massive Funding Round:** Figure AI, a startup developing humanoid robots, raised a staggering \$675 million in a Series B funding round, valuing the company at \$2.6 billion post-money. The funding round attracted prominent investors, including Jeff Bezos (through Bezos Expeditions), Microsoft, Nvidia, OpenAI Startup Fund, Amazon Industrial Innovation Fund, Intel Capital, Align Ventures, and ARK Invest.
- **Involvement of Major Tech Companies:**
  - OpenAI, the company behind ChatGPT, entered into a collaboration agreement with Figure AI to develop next-generation AI models for humanoid robots, combining OpenAI's research with Figure's robotics expertise.
  - Microsoft is investing \$95 million in Figure AI and will provide its Azure cloud services for AI infrastructure, training, and storage.
  - Nvidia, a leading chipmaker, is investing \$50 million in Figure AI.
  - Amazon's investment arm, the Intel Capital venture fund are also participating in the funding round.
- **Other Significant Investments:**
  - Norwegian startup 1X Technologies raised \$100 million in funding from OpenAI.
  - Agility Robotics, backed by Amazon in 2022, is testing its humanoid robots in Amazon warehouses.
  - Sanctuary AI is developing a humanoid robot called Phoenix.
  - Increased Interest from Venture Capital Firms: Venture capital firms like Parkway Venture Capital, Align Ventures, ARK Venture Fund,

Aliya Capital Partners, and Tamarack are investing in humanoid robotics startups. The funding landscape remains challenging, but the AI boom has given hope to startups in the humanoid robotics space.

- **Government Support:** the potential government support, especially from China, is a significant factor driving market growth

#### F. Technological and Economic Viability

##### 1) Technological Advancements:

- Integration of End-to-End AI and Multi-Modal AI Algorithms:
- The incorporation of end-to-end AI and multi-modal AI algorithms has accelerated product iterations and improved robot capabilities.
- This has enabled faster development cycles and enhancements in areas like manipulation and interaction, as seen in various products launched in 2023 (e.g., Tesla Optimus Gen 2).

##### 2) Advancements in Hardware and Supply Chain:

- Better hardware configurations and a wider, deeper manufacturing supply chain, especially in China, have contributed to technological progress.
- The availability of cheaper components and a broader scope of domestic supply chain options have driven cost reductions.
- The development of robotic LLMs, such as Google's PaLM-E, PaLI-X, and RT-2, has enabled significant advancements in natural language processing, vision, and control capabilities for humanoid robots.

##### 3) Economic Viability:

- The BOM cost for high-spec humanoid robots has likely decreased by 40% to \$150,000 per unit in 2023, down from around \$250,000 the previous year.
- This cost reduction is driven by the availability of cheaper components and a broader domestic supply chain, improving the economic feasibility of factory and consumer applications.

##### 4) Accelerated Timeline for Commercial Viability:

- Based on the cost reductions and technological advancements, factory applications could become economically viable between 2024 and 2027, one year earlier than previously expected (2025-2028).
- Consumer applications are projected to become economically viable between 2028 and 2031, 2-4 years earlier than the previous forecast (2030-2035).

##### 5) Potential Demand and Labor Substitution:

- Considering the current technological capabilities, the visible demand is identified for humanoid robots in structured environments like manufacturing (e.g., EV assembly, component sorting).
- For hazardous and dangerous tasks, such as special operations, disaster rescue, and nuclear maintenance, the customers may be willing to pay a higher price for

humanoid robots due to their adaptability enabled by AI algorithms.

- Assuming a 5-15% labor substitution rate for these applications, the global demand for humanoid robots could potentially reach 1.1 million to 3.5 million units.

#### G. Geographical trends

##### 1) Geographical Insights

The humanoid robot market is experiencing significant growth across various regions, driven by technological advancements, increasing demand for automation, and supportive government policies.

##### a) North America

- **United States:** The U.S. is a major player in the humanoid robot market, with companies like Tesla and Boston Dynamics leading the charge in robot development. The region is expected to dominate the global humanoid robot market due to robust technological ecosystems and significant investments in research and development. The U.S. market is currently estimated at \$430.8 Million.

- **Canada and Mexico:** These countries are also part of the North American market, benefiting from the technological advancements and investments in the region.

##### b) Asia-Pacific

- **China:** China is aggressively pushing for the mass production of humanoid robots with the aim of becoming a global leader in the field by 2025. The Chinese government has issued guidelines to accelerate the development of humanoid robots, focusing on key technologies such as AI, high-end manufacturing, and new materials. The country aims to establish a domestic ecosystem for humanoid robots, with products expected to be in mass production by 2025. China's market is forecasted to grow at a CAGR of 26.7%, indicating strong market potential.

- **Japan:** Japan has a long-standing tradition of integrating robotics into various industries, including manufacturing, healthcare, and entertainment. Japanese companies like Fanuc and Softbank Robotics are pioneers in the field, and the country's aging population is driving the development of robots for elderly care. Japan's market is projected to witness healthy growth rates of 17.5%.

- **South Korea:** South Korea is renowned for its innovation in humanoid robots, supported by technological expertise and government initiatives. The country is home to advanced robotics companies like the Korea Advanced Institute of Science and Technology (KAIST).

- **Other Asia-Pacific Countries:** Countries like India, Australia, Singapore, and Taiwan are also making significant strides in the humanoid robot market, driven by investments in research and development and the adoption of automation technologies.

##### c) Europe

- **Germany:** Germany is a leader in industrial robotics and automation, with a strong manufacturing base driving innovation. German companies like KUKA and Festo are at the forefront of developing intelligent robots for various industrial applications. The country's market is on track to expand at a CAGR of approximately 20.9%.
- **United Kingdom, France, and Italy:** These countries are also key players in the European humanoid robot market, benefiting from strong research institutions and investments in robotics technology.
- **Scandinavian Countries:** Denmark and Sweden are notable for their contributions to collaborative robotics and industrial automation. Companies like Universal Robots and ABB are leading the way in developing flexible and user-friendly robots.

*d) Middle East and Africa*

- **GCC Region:** The Gulf Cooperation Council (GCC) countries, particularly Saudi Arabia and the UAE, are investing heavily in robotics and automation as part of their economic diversification strategies. The region is witnessing significant growth in the adoption of humanoid robots for various applications, including healthcare and customer service.
- **Brazil and Argentina:** These countries are part of the growing South American market for humanoid robots, driven by increasing investments in automation and technological advancements.

*2) Companies in the Humanoid Robot Sector*

The humanoid robot market is characterized by a diverse range of companies spread across North America, Asia-Pacific, Europe, and other regions. Key players like Tesla, Boston Dynamics, SoftBank Robotics, and UBTECH Robotics are driving innovation and commercialization in this sector. The geographical distribution of these companies highlights the global nature of the humanoid robot market, with significant contributions from the United States, China, Japan, South Korea, and various European countries.

*3) Notable Global Humanoid Robot Brands*

- **Sophia (Hanson Robotics):** A social humanoid robot known for its ability to interact with humans and perform various tasks.
- **Pepper (SoftBank Robotics):** A semi-humanoid robot designed to read emotions and interact with humans in multiple languages.
- **Atlas (Boston Dynamics):** An advanced humanoid robot designed for real-world applications, known for its agility and mobility.
- **Digit (Agility Robotics):** A multi-purpose robot designed to navigate and perform tasks in various environments.
- **Phoenix (Sanctuary AI):** A general-purpose humanoid robot designed to perform a wide range of human tasks.

- **Optimus (Tesla):** A humanoid robot designed for industrial applications, leveraging Tesla's AI and manufacturing expertise.
- **TALOS (PAL Robotics):** A humanoid robot designed for industrial applications, known for its high-performance sensors and advanced control systems

*4) North America*

*a) United States:*

- **Tesla:** Known for its Optimus robot, Tesla is leveraging its AI and manufacturing expertise to develop humanoid robots for industrial applications.
- **Boston Dynamics:** A leader in advanced robotics, Boston Dynamics is renowned for its Atlas robot, which is designed for real-world applications.
- **Agility Robotics:** Specializes in multi-purpose robots like Digit, which are designed to navigate and perform tasks in various environments.
- **Figure AI:** Focuses on creating commercially viable autonomous humanoid robots, such as Figure 01, aimed at addressing labor shortages.
- **Promobot Corp.:** Develops service robots for public relations, personal assistance, and caregiving.
- **Kindred Inc.:** Engages in the development of AI-driven robots for various applications.
- **National Aeronautics and Space Administration (NASA):** Involved in the development of humanoid robots for space exploration and other advanced applications.

*b) Canada:*

- **Sanctuary AI:** Known for its general-purpose humanoid robot, Phoenix, which is designed to perform a wide range of human tasks.
- **Diligent Robotics:** Develops robot assistants like Moxi to support healthcare workers by handling routine tasks.

*5) Asia-Pacific*

*a) China:*

- **UBTECH Robotics:** A leading AI and humanoid robotics company, known for developing consumer and business robots.
- **Unitree Robotics:** Known for its H1 humanoid robot, which has set benchmarks in speed and agility.
- **Hanson Robotics:** Famous for its social humanoid robot, Sophia, which can interact with humans and perform various tasks.
- **Xiaomi:** Engages in the development of advanced robotics and AI technologies.

*b) Japan:*

- **SoftBank Robotics:** Known for its social robots like Pepper, which can read emotions and interact with humans.

- **Honda Motor Co., Ltd.**: Develops advanced humanoid robots for various applications.
- **Toyota Motor Corporation**: Known for its T-HR3 robot, which can be controlled remotely and is designed for safe interaction with humans.
- **Kawada Robotics Corporation**: Engages in the development of humanoid robots for industrial applications.
- **ROBOTIS**: Specializes in robotics components and systems.
- **Hajime Research Institute, Ltd.**: Focuses on advanced robotics research and development.
- **Advanced Telecommunications Research Institute International (ATR)**: Involved in cutting-edge robotics research.
- c) *South Korea:*
  - **Samsung Electronics**: Develops advanced robotics and AI technologies for various applications.
  - **HYULIM Robot Co., Ltd.**: Engages in the development of humanoid robots for industrial and commercial use.

6) *Europe*

a) *Spain:*

- **PAL Robotics**: Known for its customizable humanoid robots like TALOS, designed for industrial and commercial applications.
- **Macco Robotics**: Develops humanoid robots for the hospitality sector, focusing on food and beverage service.

b) *United Kingdom:*

- **Engineered Arts**: Known for its advanced humanoid robots like Ameca and RoboThespian, which are used for entertainment and educational purposes.
- **Shadow Robot Company**: Specializes in highly articulated robotic hands and systems.

c) *Italy:*

- **Istituto Italiano di Tecnologia (IIT)**: Engages in advanced robotics research and development.

7) *Middle East and Africa*

a) *United Arab Emirates:*

- **Various initiatives**: The region is investing in robotics and automation as part of its economic diversification strategies.

8) *South America*

a) *Brazil and Argentina:*

- **Emerging markets**: These countries are part of the growing South American market for humanoid robots, driven by increasing investments in automation and technological advancements.

#### *H. Economic Timelines for Humanoid Robots*

The economic viability and timelines for the deployment of humanoid robots have been significantly influenced by advancements in technology, cost reductions, and increasing demand for automation.

- **Base Case**: The base case scenario predicts a 53% compound annual growth rate (CAGR) from 2025 to 2035, with shipments reaching 1.4 million units by 2035. This scenario assumes continued advancements in AI and cost reductions.
- **Bull Case**: In the bull case scenario, shipments are expected to hit 1 million units by 2031, four years ahead of previous expectations, driven by accelerated advancements in end-to-end AI.
- **Blue-Sky Scenario**: In the most optimistic scenario, the market could reach up to \$154 billion by 2035, comparable to the global electric vehicle market and one-third of the global smartphone market as of 2021. This scenario assumes that all technological and market hurdles are overcome.
- **Demand for Hazardous Jobs**: The need for robots to handle dangerous jobs is elevated by national policies. Sensitivity analysis suggests global demand could reach 1.1 to 3.5 million units, assuming a 5-15% substitution rate for special operations and auto manufacturing.
- **Special Operations**: Humanoid robots are particularly appealing for special operations such as disaster rescue, nuclear reactor maintenance, and hazardous chemical industry tasks, where human willingness to perform these jobs is low.
- **Increased Investments**: There is stronger commitment from the supply chain, startups in the US and Asia, and multiple listed companies setting up new robot divisions. Government support, especially from China, is also a significant factor driving market growth.
- **Cost Curve**: The cost curve for humanoid robots has trended down faster than expected, implying better application economics and faster commercialization timelines.
- **Total Addressable Market (TAM)**: The TAM for humanoid robots is projected to reach \$38 billion by 2035, up from an initial forecast of \$6 billion. This increase is driven by a fourfold rise in shipment estimates to 1.4 million units.
- **Cost Reductions**: The Bill of Materials (BOM) cost for high-spec humanoid robots has decreased by 40% to \$150,000 per unit in 2023, down from \$250,000 the previous year. This reduction is due to the availability of cheaper components and a broader domestic supply chain.
- **Factory Applications**: The timeline for factory applications has been accelerated by one year, now expected to be economically viable between 2024 and 2027, compared to the previous estimate of 2025 to 2028.

- **Consumer Applications:** The timeline for consumer applications has also been accelerated by 2-4 years, now expected to be economically viable between 2028 and 2031, compared to the previous estimate of 2030 to 2035.

### I. Technology progress in Humanoid Robots

Progress in both hardware and software, including the development of LLMs and end-to-end AI, has significantly advanced the capabilities of humanoid robots. These advancements are paving the way for humanoid robots to become more integrated into various aspects of daily life and industry, offering promising prospects for the future of robotics.

#### 1) Hardware Progress in Humanoid Robots

The development of humanoid robots has seen remarkable advancements in hardware, making these robots more versatile, efficient, and capable of performing complex tasks.

- **Bipedal Mobility and Dexterity:** Humanoid robots have achieved significant improvements in bipedal mobility, allowing them to navigate complex environments with agility and precision. For instance, Agility Robotics' Digit exemplifies this progress with its ability to move and walk on two feet, showcasing the potential for robots to assist in areas previously considered too challenging for automation. Similarly, advancements in dexterity, particularly in the manipulation of objects, have been noted, although this remains an area with room for improvement.
- **Sensory Perception and Feedback Systems:** The integration of advanced sensors and feedback systems has enabled humanoid robots to better perceive and interact with their surroundings. These developments have paved the way for increased autonomy and interaction capabilities, allowing robots to observe and react to their environment more effectively.
- **Component Cost Reduction:** There has been a significant reduction in the cost of components necessary for building humanoid robots, such as high-precision gears, actuators, and batteries. This cost reduction is primarily due to the availability of cheaper components, more supply chain options, and improvements in design and manufacturing techniques. For example, the manufacturing cost of humanoid robots has dropped from a range of \$50,000-\$250,000 per unit to \$30,000-\$150,000, facilitating faster commercialization.

#### 2) Software Progress in Humanoid Robots

Software advancements have been equally pivotal in the evolution of humanoid robots, with significant progress in areas such as:

- **Large Language Models (LLMs):** The development of robotic LLMs, such as Google's PaLM-E and RT-2, has been a key factor in advancing humanoid robots. These models enhance the robots' ability to process natural language commands and analyze tasks' scenarios through vision, enabling them to execute tasks with a level of understanding and responsiveness akin to human perception.
- **End-to-End AI:** The shift towards end-to-end AI, where models can train themselves without the need for manual coding by engineers, has accelerated robot

development. This approach allows robots to adapt to new situations more quickly and perform a wider range of tasks. Tesla's Optimus Gen 2 is an example of a humanoid robot benefiting from end-to-end AI, demonstrating rapid product iteration and the ability to perform tasks autonomously.

#### 3) Robotic LLMs development

- **Introduction of PaLM-E and RT-2:** 2023 saw significant advancements in robotic LLMs with the introduction of PaLM-E and RT-2. These models represent a leap forward in integrating AI with robotics, enabling robots to understand and interact with their environment in more sophisticated ways.
- **PaLM-E's Multimodal Capabilities:** PaLM-E, developed by Google, is an embodied multimodal language model designed for robotics. It combines the power of large language models with the ability to process visual and sensor data, enabling robots to perform tasks across multiple modalities. PaLM-E's architecture allows it to understand and execute tasks on various types of robots and for multiple modalities, including images, robot states, and neural scene representations.
- **RT-2's Vision-Language-Action Model:** RT-2, or Robotics Transformer 2, developed by Google DeepMind, is a vision-language-action (VLA) model that learns from both web and robotics data. It translates high-level reasoning into low-level machine-executable instructions, significantly enhancing robots' ability to manage unforeseen situations and making them more versatile as all-purpose machines.
- **Impact on Robotics:** The development of PaLM-E and RT-2 has profound implications for the field of robotics. These models enable robots to perform tasks with a higher degree of autonomy and adaptability, bridging the gap between AI's theoretical capabilities and practical applications in robotics.

#### 4) End-to-End AI in Robotics

The integration of LLMs and end-to-end AI in robotics has led to:

- **Enhanced Human-Robot Interaction:** LLMs and end-to-end AI have significantly improved human-robot interaction, making robots more capable of understanding and responding to human commands in a natural and intuitive manner. This has opened up new possibilities for humanoid robots in various industries and settings.
- **Accelerated Learning and Adaptation:** These technologies have enabled humanoid robots to learn from experiences and adapt to new tasks more efficiently. The RT-X project, for instance, aims to pool data and resources from multiple robotics labs to create versatile, general-purpose robots that can operate effectively beyond limited lab settings.
- **Increased Autonomy:** The advancements in LLMs and end-to-end AI have contributed to the increased autonomy of humanoid robots, allowing them to perform complex tasks with minimal human intervention. This autonomy is crucial for deploying humanoid robots in real-world applications where human-like interaction and adaptability are essential.

### J. Industry insights

Humanoid robots offer significant potential benefits for military applications, including enhanced capabilities, operational efficiency, and cost savings. However, their deployment also raises ethical, legal, and technical challenges that must be carefully managed. The economic benefits of investing in humanoid robots are substantial, with potential gains in productivity, scalability, and long-term technological advancements. As technology continues to evolve, it will be crucial to address the associated risks and ensure that the deployment of humanoid robots in the military is conducted responsibly and ethically.

#### 1) Current Uses of Humanoid Robots

- **Manufacturing:** Humanoid robots are used in manufacturing for tasks such as assembly, quality control, and material handling. They can perform repetitive tasks with high precision and can work in environments that may be hazardous to humans.
- **Healthcare:** In healthcare, humanoid robots assist with patient care, rehabilitation, and surgery. They can monitor vital signs, assist in physical therapy, and even perform complex surgical procedures.
- **E-commerce and Warehousing:** Humanoid robots are employed in e-commerce and warehousing to handle logistics, such as sorting and transporting goods. They help improve efficiency and reduce labor costs.
- **Customer Service and Hospitality:** Humanoid robots are used in customer service roles, such as concierges, receptionists, and guides. They can interact with customers, provide information, and enhance the customer experience.
- **Security:** Humanoid robots are used in security to patrol areas, detect intrusions, and monitor for safety hazards. They can operate continuously without fatigue and provide real-time data to human operators.
- **Education and Research:** In educational settings, humanoid robots are used as teaching aids and research tools. They help students learn about robotics, programming, and artificial intelligence.
- **Entertainment:** Humanoid robots are also used in entertainment, such as performing at events, acting as tour guides in museums, and even conducting orchestras
- *Potential Future Uses of Humanoid Robots*
- **Military:** Humanoid robots could be used in military applications for tasks such as reconnaissance, bomb disposal, and logistics support. They can operate in dangerous environments, reducing the risk to human soldiers.
- **Cyberbiosecurity:** Humanoid robots could play a role in cyberbiosecurity by monitoring and protecting biological data and systems from cyber threats. Their advanced sensors and AI capabilities make them suitable for this role.
- **Oil and Gas Industry:** In the oil and gas industry, humanoid robots could be used for inspection, maintenance, and repair of offshore platforms and pipelines. They can operate in hazardous environments, reducing the need for human intervention.

- **Mining:** Humanoid robots could be used in mining to perform tasks such as drilling, ore extraction, and safety inspections. They can work in dangerous and confined spaces, improving safety and efficiency.
- **Financial Services and Stock Markets:** Humanoid robots could assist in financial services by providing customer support, conducting transactions, and analyzing market data. Their ability to process large amounts of information quickly makes them valuable in this sector.
- **Real Estate Development:** In real estate, humanoid robots could be used for property inspections, maintenance, and customer interactions. They can provide virtual tours and assist with property management tasks.
- **Food and Grocery Industry:** Humanoid robots could be used in the food and grocery industry for tasks such as stocking shelves, preparing food, and delivering groceries. They can help improve efficiency and reduce labor costs.
- **Aircraft:** In the aircraft industry, humanoid robots could assist with maintenance, inspections, and assembly of aircraft components. Their precision and ability to work in confined spaces make them suitable for this role.
- **Maritime and Shipping:** Humanoid robots could be used in maritime and shipping for tasks such as cargo handling, ship maintenance, and safety inspections. They can operate in harsh marine environments, improving efficiency and safety.
- **Smart Cities:** In smart cities, humanoid robots could be used for various tasks such as traffic management, public safety, and maintenance of infrastructure. They can interact with citizens, provide information, and help manage urban environments.

#### 2) Industry implications detailed

##### a) Military

- **Benefits:** Enhanced safety for military personnel by performing dangerous tasks, such as bomb disposal and reconnaissance missions, without risking human lives.
- **Risks:** Potential for increased lethality and ethical concerns regarding autonomous decision-making in combat situations.
- **Applications:** Combat support, search and rescue operations, and logistics.
- **Economic Benefits:** Reduction in training and healthcare costs associated with human soldiers.

##### b) Cyberbiosecurity

- **Benefits:** Improved security protocols in handling sensitive biological data and materials, reducing the risk of biohazards.
- **Risks:** Vulnerability to hacking and misuse, potentially leading to biosecurity threats.
- **Applications:** Secure handling and analysis of biohazardous materials, surveillance of biosecure areas.

- **Economic Benefits:** Enhanced efficiency in biosecurity management, potentially reducing the costs associated with biosecurity breaches.
- c) *Oil and Gas Industry*
  - **Benefits:** Increased safety by performing hazardous tasks such as drilling and pipeline inspections, reducing workplace accidents.
  - **Risks:** High initial investment costs and potential job displacement.
  - **Applications:** Automated drilling, maintenance, and inspection of offshore platforms and pipelines.
  - **Economic Benefits:** Operational efficiency and reduced downtime, leading to cost savings.
- d) *Mining (Metal, Gold, etc.)*
  - **Benefits:** Enhanced safety in dangerous mining environments and increased operational efficiency.
  - **Risks:** Job displacement and reliance on technology that may malfunction in remote or harsh conditions.
  - **Applications:** Exploration, drilling, and ore processing in hazardous or inaccessible areas.
  - **Economic Benefits:** Improved productivity and reduced operational costs through automation.
- e) *Financial Services and Stock Markets*
  - **Benefits:** Improved accuracy and speed in data analysis and decision-making processes.
  - **Risks:** Potential for algorithmic biases and financial market manipulation.
  - **Applications:** Automated trading, risk assessment, and customer service.
  - **Economic Benefits:** Increased market efficiency and reduced operational costs.
- f) *Real Estate Development*
  - **Benefits:** Enhanced project planning and execution through precise measurements and labor.
  - **Risks:** High initial costs and potential for errors in complex development projects.
  - **Applications:** Site inspections, construction tasks, and customer interaction in sales centers.
  - **Economic Benefits:** Streamlined development processes and reduced labor costs.
- g) *Food and Grocery Industry e-commerce*
  - **Benefits:** Improved efficiency in order fulfillment and inventory management.
  - **Risks:** Potential loss of jobs and challenges in handling delicate products.
  - **Applications:** Automated picking and packing, customer service, and inventory audits.
- h) *Aircraft*
  - **Benefits:** Precision in manufacturing processes and maintenance tasks.
  - **Risks:** High development costs and potential for errors in critical safety systems.
  - **Applications:** Assembly, inspection, and repair of aircraft components.
  - **Economic Benefits:** Reduced manufacturing and maintenance costs, improved safety records.
- i) *Manufacturing*
  - **Benefits:** Increased production efficiency and flexibility in handling diverse tasks.
  - **Risks:** Job displacement and initial investment costs.
  - **Applications:** Assembly lines, quality control, and logistics.
  - **Economic Benefits:** Enhanced productivity and reduced labor costs.
- j) *Healthcare*
  - **Benefits:** Assistance in surgeries, patient care, and rehabilitation with precision and consistency.
  - **Risks:** Ethical concerns regarding patient interaction and potential for malfunctions.
  - **Applications:** Surgical assistance, patient monitoring, and physical therapy.
  - **Economic Benefits:** Improved patient outcomes and potential reduction in healthcare costs.
- k) *Maritime and Shipping*
  - **Benefits:** Enhanced safety in hazardous conditions and improved efficiency in cargo handling.
  - **Risks:** Navigational errors and potential for piracy or hijacking.
  - **Applications:** Cargo loading and unloading, ship maintenance, and at-sea inspections.
  - **Economic Benefits:** Reduced operational costs and improved turnaround times.
- l) *Smart City*
  - **Benefits:** Improved public services and safety through surveillance and maintenance tasks.
  - **Risks:** Privacy concerns and high implementation costs.
  - **Applications:** Public space maintenance, waste management, and security patrols.
  - **Economic Benefits:** Enhanced quality of life for residents and potential attraction for businesses.

Read more: [Boosty](#) | [Sponsr](#) | [TG](#)



STARRY SECURITY