MSECB

Risk Based Governance in the AI Era, How ISO/IEC 27001 and ISO/IEC 42001 Complement Each Other

By:

- *Adel Abdelmoneim*
- *Mostafa Alshamy*

MSECB

Webinar Agenda

- Risk based governance
- AI risks and how to manage them
- Q&A

MSECB

Background of
Adel Abdel Moneim

Registered cybersecurity expert with ITU-ARCC With 28+ years of experience, he has been a pioneer in the cybersecurity field—particularly in ethical hacking and penetration testing—while leading major projects across multiple critical sectors.

Recognized as one of the Middle East's foremost GRC leaders, Adel brings deep expertise in globally respected frameworks and standards, including ISOs, NIST,TOGAF, COBIT & SABSA.

Adel is accredited Trainer by ISC2, ISACA, EC-Council, APMG, PECB, and CertNexus. is also a Certified MSECB Auditor for numerous ISO standards as well as a CSA Star Certification.

Globally recognized as a Top Cybersecurity Influencer (IFSEC Global 2019–2021), Adel continues to be a trusted advisor on cybersecurity strategies, policies, and awareness initiatives across the Middle East and beyond

MSECB

Background of Mostafa AlShamy

Mostafa AlShamy is a trainer, assessor, consultant, and then auditor with more than 20 years of experience in GRC and respective fields, including but not limited to SMS, ISMS/PIMS, BCMS, RM, Data Governance, and Management.

In the last eight years, he has conducted tens of audits on behalf of MSECB over four continents. Through his experience, he has helped many organizations express their commitment to quality and continuous improvement.

malshamy@ofouqis.com
https://www.linkedin.com/in/malshamy/

MSECB

About MSECB

- MSECB is an IAS-accredited certification body for management systems on various international standards.
- Furthermore, MSECB, as a Corporate Member of the Cloud Security Alliance (CSA), offers Level 2 STAR Certification in conjunction with ISO/IEC 27001.
- We are also proud members of the Independent Association of Accredited Registrars (IAAR), a member-driven organization promoting accredited management system certification.

Independent Association of Accredited Registrars

IAS ACCREDITED Management Systems Certification Body MSCB-111

ACCREDIA

cloud security alliance®

MSECB

What is Governance and How is it Based?

Definition: Governance refers to the system of rules, practices, and processes by which an organization is directed and controlled. It provides the framework for achieving a company's objectives and ensures accountability and transparency.

Core Components of a Governance Framework:

- **Understanding the Context (Where we are):** A thorough evaluation of the organization's internal and external environment. This includes identifying stakeholders, their expectations, and the regulatory landscape.
- **Directing Management (Where we are going):** The board and senior leadership set the strategic direction and objectives. This involves establishing policies, defining roles and responsibilities, and allocating resources.
- **Monitoring Performance (Corrective Actions):** Regularly tracking progress towards objectives and making necessary adjustments. This includes internal audits, performance evaluations, and compliance checks to ensure the governance framework is effective.

MSECB

How Governance is Based on Risks

Risk-Based Governance: This approach integrates risk management into the overall governance framework. It ensures that an organization's strategy and decision-making processes are informed by a clear understanding of its significant risks.

- **Key Principles:**
- **Proactive Risk Identification:** Instead of reacting to issues as they arise, a risk-based approach proactively identifies potential threats and opportunities.
- **Prioritization:** It allows organizations to focus resources on the most critical risks that could impact their objectives.
- **Informed Decision-Making:** By understanding the potential impact of risks, leadership can make more strategic and informed decisions.
- **Enhanced Resilience:** Proactively managing risks enhances an organization's ability to withstand and recover from adverse events.

MSECB

ISO Annex SL - The Foundation for Modern Management System Standards

What is Annex SL?

Annex SL provides a high-level structure (HLS) for all new and revised ISO management system standards. Its purpose is to enhance consistency and alignment between different standards, making it easier for organizations to implement multiple management systems.

Key Elements of the Annex SL Structure:

1. Scope
2. Normative References
3. Terms and Definitions
4. Context of the Organization
5. Leadership
6. **Planning (Addresses Risks and Opportunities)**
7. Support
8. Operation
9. Performance Evaluation
10. Improvement

Risk Management is a Core Component: Clause 6 on "Planning" explicitly requires organizations to identify, analyze, and plan actions to address risks and opportunities. This risk-based approach is fundamental to both ISO 27001 and ISO 42001.

MSECB

A Brief History of the AI Era

The concept of artificial intelligence has a long history, with significant acceleration in recent decades.

- **The Birth of AI (1950s):** The term "artificial intelligence" was coined by John McCarthy in 1956. Early work focused on problem-solving and symbolic methods. The Turing Test was proposed as a measure of a machine's ability to exhibit intelligent behavior.
- **AI Maturation and Expert Systems (1960s-1980s):** Development of early chatbots like ELIZA and the first mobile robot, Shakey. The 1980s saw a boom in "expert systems" designed to mimic the decision-making ability of a human expert in a specific domain.
- **The Rise of Machine Learning (1990s-2000s):** A shift towards statistical learning methods and the availability of large datasets fueled advancements in machine learning.
- **Deep Learning and the Modern AI Boom (2010s-Present):** The introduction of deep learning architectures, particularly neural networks, led to breakthroughs in areas like image recognition, natural language processing, and generative AI.

MSECB

Risks Covered by ISO/IEC 27001 and ISO/IEC 42001

While both standards address risk, their focus areas are distinct yet complementary.

ISO/IEC 27001 (Information Security): Focuses on protecting the confidentiality, integrity, and availability of information. Key risks include:

- Unauthorized access to sensitive data
- Cyber-attacks such as malware and phishing
- Data breaches and leakage
- Insider threats
- System vulnerabilities and failures
- Etc.

MSECB

Risks Covered by ISO/IEC 27001 and ISO/IEC 42001 Cont.

While both standards address risk, their focus areas are distinct yet complementary.

- **ISO/IEC 42001 (Artificial Intelligence):** Addresses the unique risks associated with AI systems. These include:
- **Bias and Fairness:** AI models producing discriminatory or unfair outcomes.
- **Transparency and Explainability:** Difficulty in understanding how an AI system makes its decisions.
- **Accountability:** Determining who is responsible for the actions of an AI system.
- **Privacy:** AI systems processing large amounts of personal data.
- **Security of AI Systems:** Vulnerabilities specific to AI, such as model evasion or data poisoning.
- **Societal and Ethical Impacts:** Broader consequences on society, including job displacement and misinformation.

MSECB

ISO/IEC 27001's Risk-Based Approach to the ISMS Scope

The latest version of ISO/IEC 27001 emphasizes that the scope of the Information Security Management System (ISMS) must be determined based on the results of a comprehensive information security risk assessment.

- **Clause 4.3: Determining the scope of the ISMS:** Requires the organization to define the boundaries and applicability of the ISMS to establish its scope.
- **Clause 6.1.2: Information security risk assessment:** Mandates a process to identify risks associated with the loss of confidentiality, integrity, and availability of information within the scope of the ISMS.
- **Clause 6.1.3: Information security risk treatment:** Requires the selection of appropriate risk treatment options. The controls listed in Annex A are a key part of this process.
- This means the entire ISMS is built upon a foundation of understanding and mitigating information security risks.

MSECB

How ISO/IEC 27001Cover Risks

- **Systematic Risk Management Process:** Requires organizations to establish, implement, maintain, and continually improve a risk management process.
- **Annex A Controls:** Provides a comprehensive set of 93 controls in the latest version (ISO/IEC 27001:2022) to address identified risks across various domains like access control, cryptography, and incident management.
- **Statement of Applicability (SoA):** Requires organizations to document which Annex A controls are applicable and justify any exclusions, directly linking controls to the risk assessment.

MSECB

How ISO/IEC 42001 Cover Risks Cont.

- **AI Risk Assessment:** Mandates a specific process to identify and analyze risks related to AI systems, considering their potential consequences for the organization and society.
- **AI Impact Assessment:** Requires an evaluation of the impact of AI systems on individuals and society.
- **AI-Specific Controls:** Provides a set of controls in its Annexes to address AI-specific risks such as data quality for AI, model transparency, and accountability.
- **Lifecycle Approach:** Enforces a structured risk management process throughout the entire lifecycle of an AI system, from design and development to deployment and decommissioning.

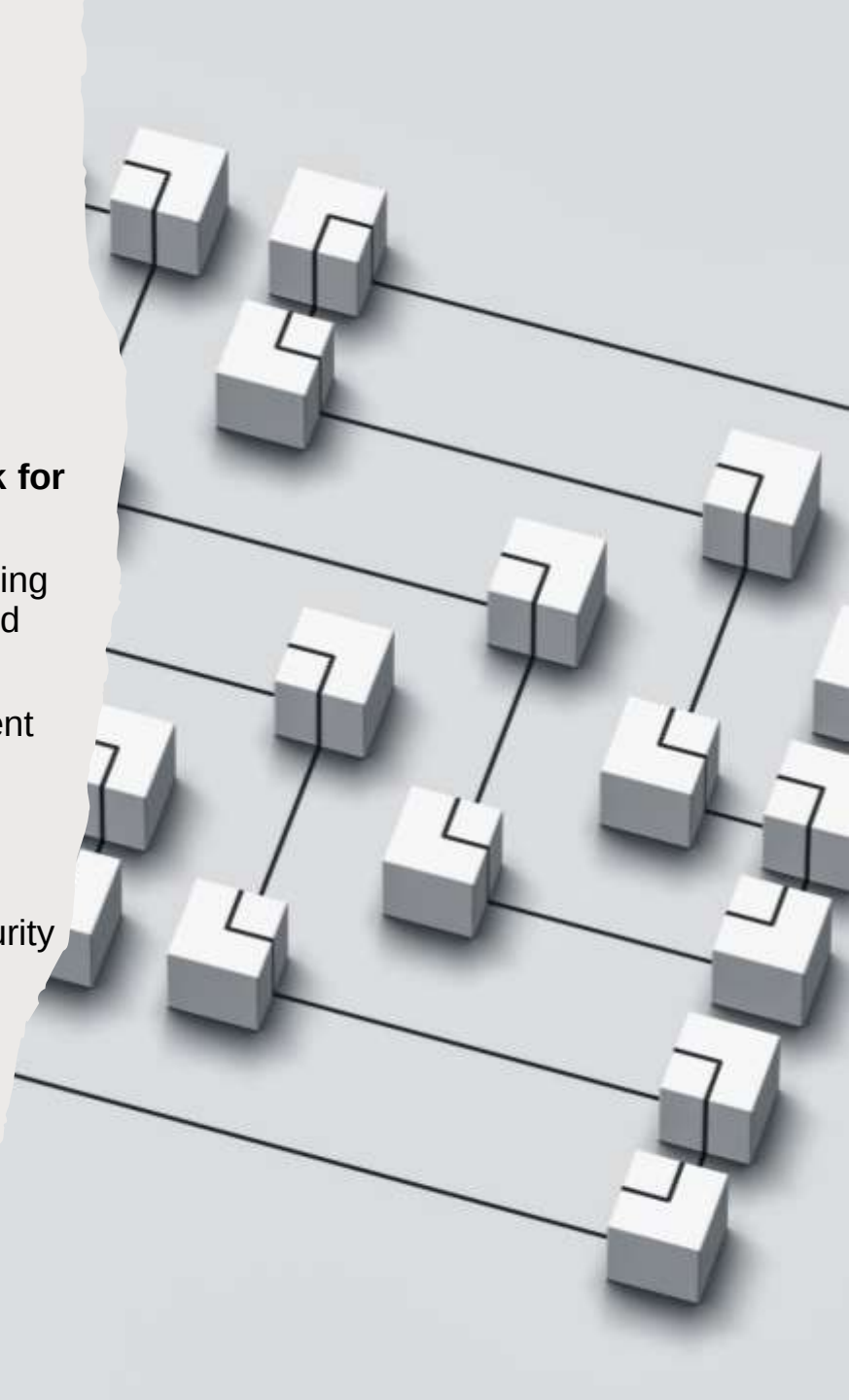
MSECB

Integrating ISO/IEC 27001 and ISO/IEC 42001

Integrating these two standards creates a powerful and comprehensive governance framework for the AI era.

- **Shared High-Level Structure (Annex SL):** Both standards are based on the same structure, making integration more straightforward. They share common clauses for context, leadership, planning, and other key areas.
- **Unified Risk Management:** Organizations can extend their existing ISO/IEC 27001 risk assessment methodologies to incorporate the specific risks associated with AI, as required by ISO/IEC 42001.
- **Leveraging Existing Controls:** Many of the information security controls in ISO/IEC 27001 are foundational for securing AI systems. ISO/IEC 42001 builds upon this with its AI-specific controls.
- **Comprehensive Governance:** An integrated approach ensures that both general information security risks and the unique challenges of AI are managed in a cohesive and ethical manner.

- **Benefits of Integration:**
- Enhanced security posture for both data and AI applications.
- Improved regulatory compliance with data protection and AI-related laws.
- Increased trust from customers and stakeholders.
- A competitive advantage by demonstrating responsible AI governance.



MSECB

A Brief Explanation of Certification Journey

MSECB

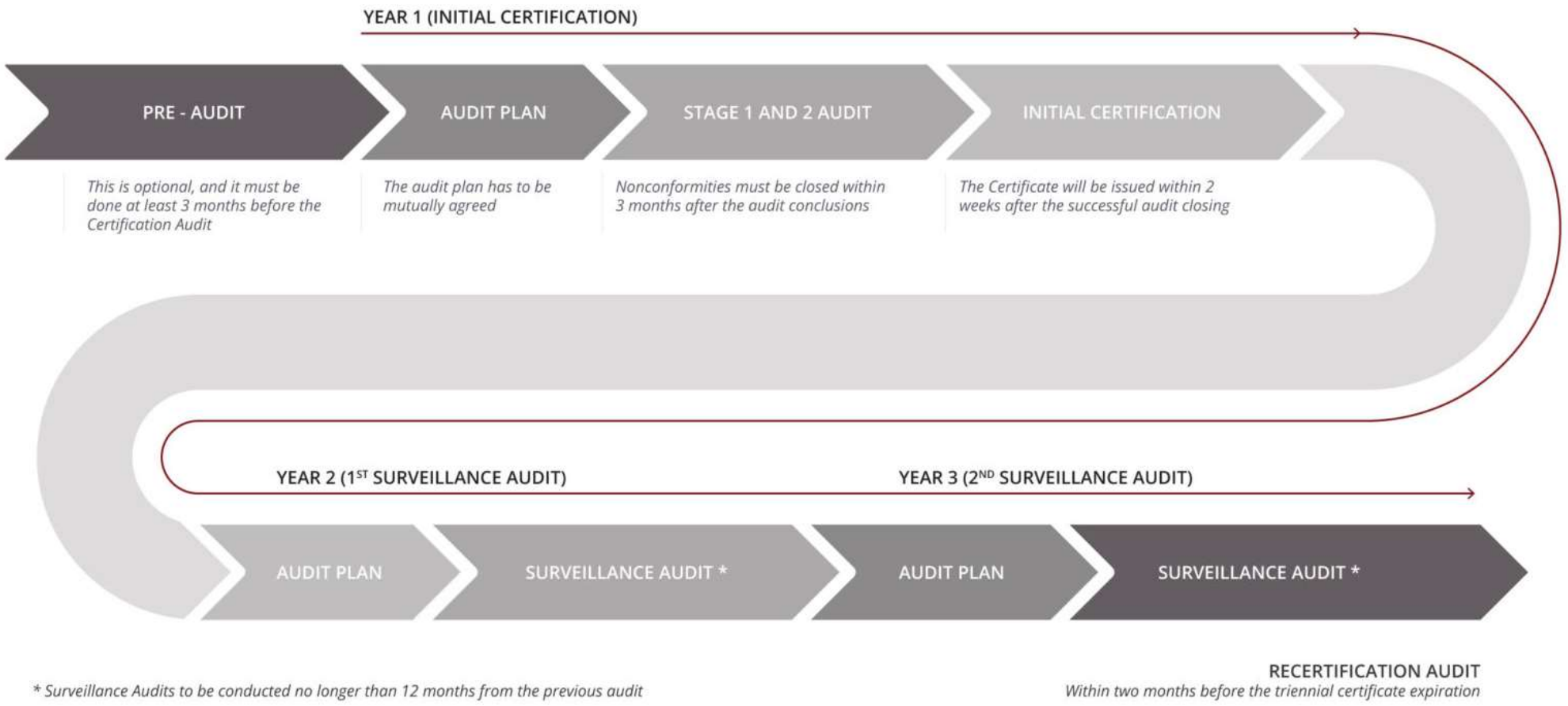
Prior Certification Journey

Organizations have a lot of work to do before the certification audit, including but not limited to:

1. Obtain management support for Management System (MS) lifecycle
2. Define scope and management intention after reviewing your organization's service catalogue
3. Identify requirements and responsibilities
4. Develop training and awareness programs
5. Design the process of risk management and perform risk assessment and treatment
6. Build the MS and implement all required controls
7. Operate the MS
8. Conduct internal audits
9. Perform management review

MSECB

MSECB's Certification Journey



* Surveillance Audits to be conducted no longer than 12 months from the previous audit

MSECB

Post Certification Journey

Organizations have a lot of work to do to update the MS accordingly after the certification audit, including but not limited to:

1. MS components continual improvement
2. MS objectives and KPIs continual measurement
3. Internal audit (at least once per year)
4. Management review (at least once per year)
5. Continuous awareness and training
6. Managing MS changes (MS is dynamic and not static)
7. Etc…

MSECB

Pitfalls to Avoid

MSECB

Pitfalls to Avoid: Prior Certification Journey

- Wrong scope (locations, DRS, branches, services, functions, …)
- Wrong type of personal data to cover (employees, customers, or both)
- Partial personal data lifecycle
- Forget consent and announcements in addition to regulators
- Not prepared for incidents and breaches
- Not sufficient or proper training or awareness
- Discover risks and forget opportunities
- Not unified Document Management System (DMS)(structure, validity, review,..Ect)
- Self-internal audit (Who shall conduct it, when, and what are the criteria?)
- Management review for technical aspects
- Paying the audit fees means having the certificate for sure

MSECB

Pitfalls to Avoid: Post Certification Journey

- Improper certification announcement
- Misunderstanding certification for regulatory compliance
- Neglecting MS regular maintenance activities including documented information review and update
- Lacking MS continuous improvement
- Neglecting last audit nonconformities and corrective actions
- 1st Surveillance shall be before 12 months from the certification audit; 2nd Surveillance before 24 months, and Recertification before 36 months.

MSECB

Groups affected by the potential harms of AI

- Who is affected?
- Individuals (civil rights, economic opportunity, safety)
- Groups (discrimination towards subgroups)
- Society (democratic process, public trust in governmental institutions, educational access, jobs
- redistribution)
- Organizations (reputational, cultural, economic, acceleration risks)
- Ecosystems (natural resources, environment, supply chain)

Resource:

What are the risks from Artificial Intelligence? https://airisk.mit.edu

MSECB

Individual harms

- Bias and discrimination
- Implicit bias
- Sampling bias
- Temporal bias
- Overfitting to training data

MSECB

Individual harms

Bias and discrimination

Bias in AI systems can cause harm to a person's civil liberties, rights, safety and economic opportunity.

Individuals developing the systems can have bias; this should be addressed during the lifecycle of AI

system development.

Implicit bias: Discrimination or prejudice toward a particular group or individual

Sampling bias: Data gets skewed toward a subset of a group and therefore may favor that subset of a

larger group

Temporal bias: A model is trained and functions properly at the time, but may not work well at a

future point, requiring new ways to address the data

Overfitting to training data: A model works for the training data, but does not work for new data

because it is so fitted to the training data

MSECB

Individual harms

Bias and discrimination
Employment and hiring
Insurance and social benefits
Housing
Education
Credit

MSECB

Individual harms

Bias and discrimination

Employment and hiring discrimination

- AI-based systems used for recruiting and hiring
- If the system is biased, it may discriminate against applicants based on gender, race, ethnicity or economic status
- Amazon, 2014: implemented an AI system to help with recruiting and hiring; during testing they found the system was biased against women
- This happened because the system was trained on test data of the resumes of men only
- Engineers tried to retrain the system, but this is difficult to do once the model has already been trained a certain way; project was eventually abandoned in 2017

Insurance and social benefit discrimination

- If the system is not appropriately modeled and developed, there can be a discriminatory impact against particular groups of individuals, often based on economic status
- Bias and discrimination (cont.)
- Housing discrimination
- Tenant selection and mortgage qualification can be affected if a biased AI system is used

Education discrimination

- AI systems used to select individuals to attend a school
- A biased system can discriminate against qualified individuals based on race, gender or economic background

Credit discrimination

- Financial lending discrimination and individuals unable to get loans
- Differential pricing of goods and services

MSECB

Individual harms

Civil rights and privacy concerns
Personal data used for AI training
Appropriation of personal data for model training
Interference
Lack of transparency of use
Inaccurate models

MSECB

Individual harms

Civil rights and privacy concerns

- Personal data used as part of AI training data
    - Screen out personal data: If you don't need personal data, it should not be used in the system;
    - personal data could be shared with individuals who should not have access to it if it is part of the larger set of data used to train the system
    - Deidentification: removing identifiers from the data, such as name, address, Social Security number; however, it is possible to reidentify an individual if data is aggregated or combined with another data set
    - With AI systems, massive amounts of data are used and there are typically multiple data sets; easy to recombine personal data from different datasets and take deidentified data, combine it with identified data, and reidentify individuals, leading to privacy issues

Appropriation of personal data for model training

- Models being trained in AI from large sources of data
- Data may come from social media or large datasets with information about individuals; individuals may have consented for one particular use of their data, but not for training an AI system

Inference: An AI system model that makes predictions or decisions

- In some cases, the systems can be used to identify individuals, but they are not always accurate
- Personal data can be attributed to the wrong individual

Lack of transparency of use

- AI systems should notify individuals when AI is being used (e.g., interacting with chatbots)

Inaccurate models

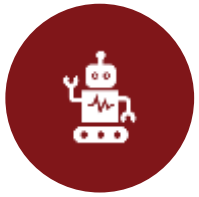
- Data accuracy is very important; AI systems are only as good as the data that trains them

Resource: The Intersection of Privacy and AI Governance, IAPP Resource Center
https://iapp.org/resources/article/the-intersection-of-privacy-and-ai-governance

MSECB

Individual harms

Economic opportunity and job loss



While AI can help to create some opportunities for jobs (increased productivity, lower costs, work assistance, possibility to create new types of future jobs), it also has the potential to affect job loss

AI being used to conduct jobs previously handled by humans (e.g., code development)

AI-driven discriminatory hiring practices

Job opportunities may fail to reach key demographics due to AI-driven tools for job targeting, marketing or hiring

If there is bias built into the AI model and it is used for marketing and recruiting people for jobs, certain demographic groups may not be contacted if that bias is toward those subgroups

MSECB

Group harms

- Facial recognition
- Mass surveillance
- Civil rights
- Deepening of racial and socio-economic divides

MSECB

Group harms

Facial recognition algorithms: Many AI systems using face recognition exhibit demographic differentials (the ability to match two images of the same person vary from one demographic group to another)

A NIST study found AI facial recognition systems to be unreliable across many kinds of systems Studies have found those with darker skin tones and females are much more difficult to recognize, leading to discrimination and bias

AI facial recognition software used by the London police once showed an 81% inaccuracy rate; can lead to biased policing, as well as the ability to track individuals online that could lead to discrimination using those types of systems

Mass surveillance: A large potential harm, particularly for marginalized groups If mass surveillance is used, protected groups or those harmed in the past may not receive as much privacy protection and may be targeted for surveillance (due to race, religion, sexual orientation, etc.)

Civil rights

Harms to freedom of assembly and protest due to tracking and profiling individuals linked to certain beliefs or actions

Deepening of racial and socio-economic divides

Discrimination against population subgroups

Mistrust among groups

MSECB

Societal harms

- Spread of disinformation
- Ideological bubbles
- Deepfakes
- Safety

MSECB

Societal harms

Societal harms are harms to the democratic process and participation.

Spread of disinformation

- Ideological bubbles or echo chambers
- Individuals exposed only to information that agrees with information they encountered in the past
- Unable to see differing views or understand broader societal implications
- Causes isolation and more division; groups only exposed to their specific ideas and values

Deepfakes: Audio, video or images manipulated to create an alternate reality

- Harmful in elections

Safety

- Lethal autonomous weapons that identify targets to attack
- Concern that without sufficient oversight, systems could evolve and may be able to attack randomly without being monitored

MSECB

Environmental harms

Carbon footprint of AI

Drain on natural resources

MSECB

Environmental harms

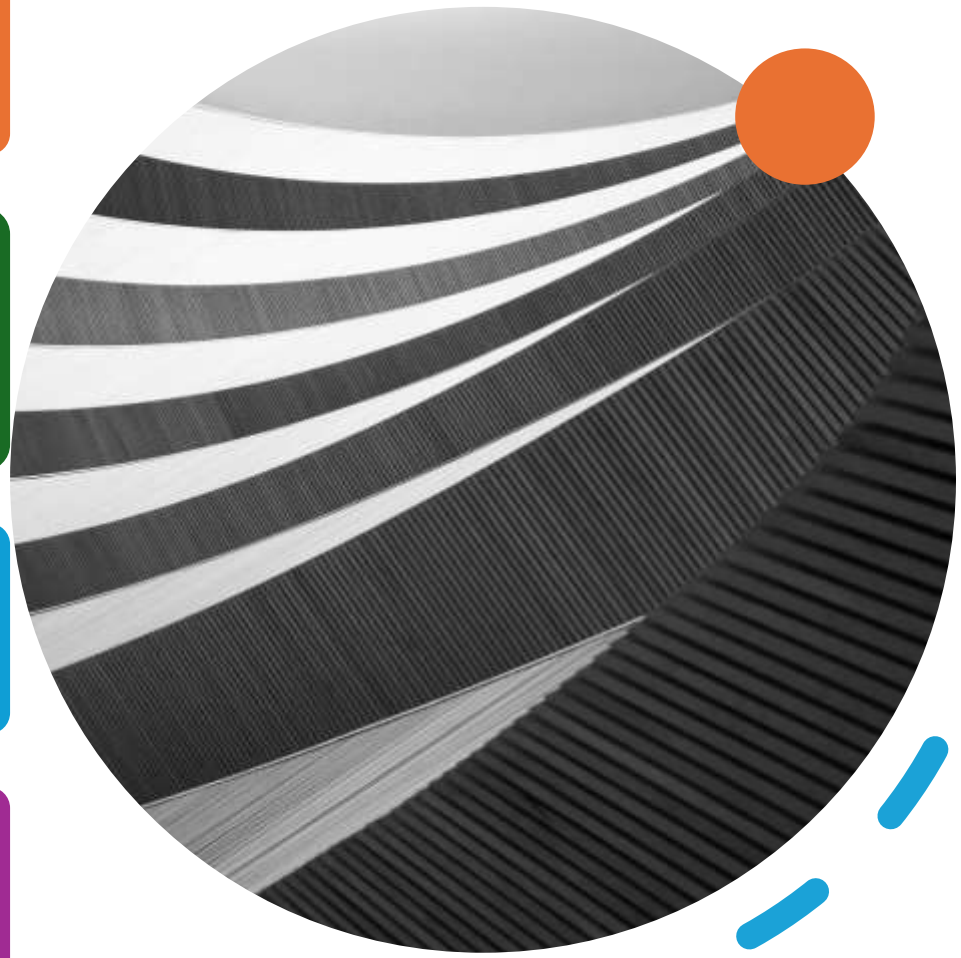
When training several common large AI models, studies found that they emit more than 626,000 pounds of carbon dioxide (the equivalent of five times the lifetime emissions of an American car)

Another study found that when looking at the top four natural language processing models, the energy consumed over the training process matches the energy mix used by Amazon's AWS, the largest cloud service provider

An additional study found that each casual use of generative AI is like dumping out a small bottle of water on the ground

To address this, many organizations are seeking alternatives to the use of electrical power

- Possibility of using batteries to power systems; this can also have an environmental impact
- E.g., lithium batteries: lithium extraction demands enormous water usage



MSECB

Organizational harms

RISKS

REPUTATIONAL

CULTURAL

ECONOMIC

ACCELERATION

LEGAL AND REGULATORY

MSECB

Organizational harms

Reputational

- Loss of customers and renewals
- Increased queries due to concerns about AI usage
- New customer concerns over AI usage
- Negative brand impact
- Share price drop and investor flight
- Company is a target for activists

Cultural

- Assumption that AI is more accurate than humans, so we are less likely to challenge its outcomes, even though AI is created by humans
- Built-in bias that AI is technology and data-driven and therefore can produce a superior outcome, which is not necessarily the case

Economic

- Costs of internal resources and remediation if something goes wrong with the AI
- Litigation costs, including class actions and punitive damages

MSECB

Organizational harms

Acceleration

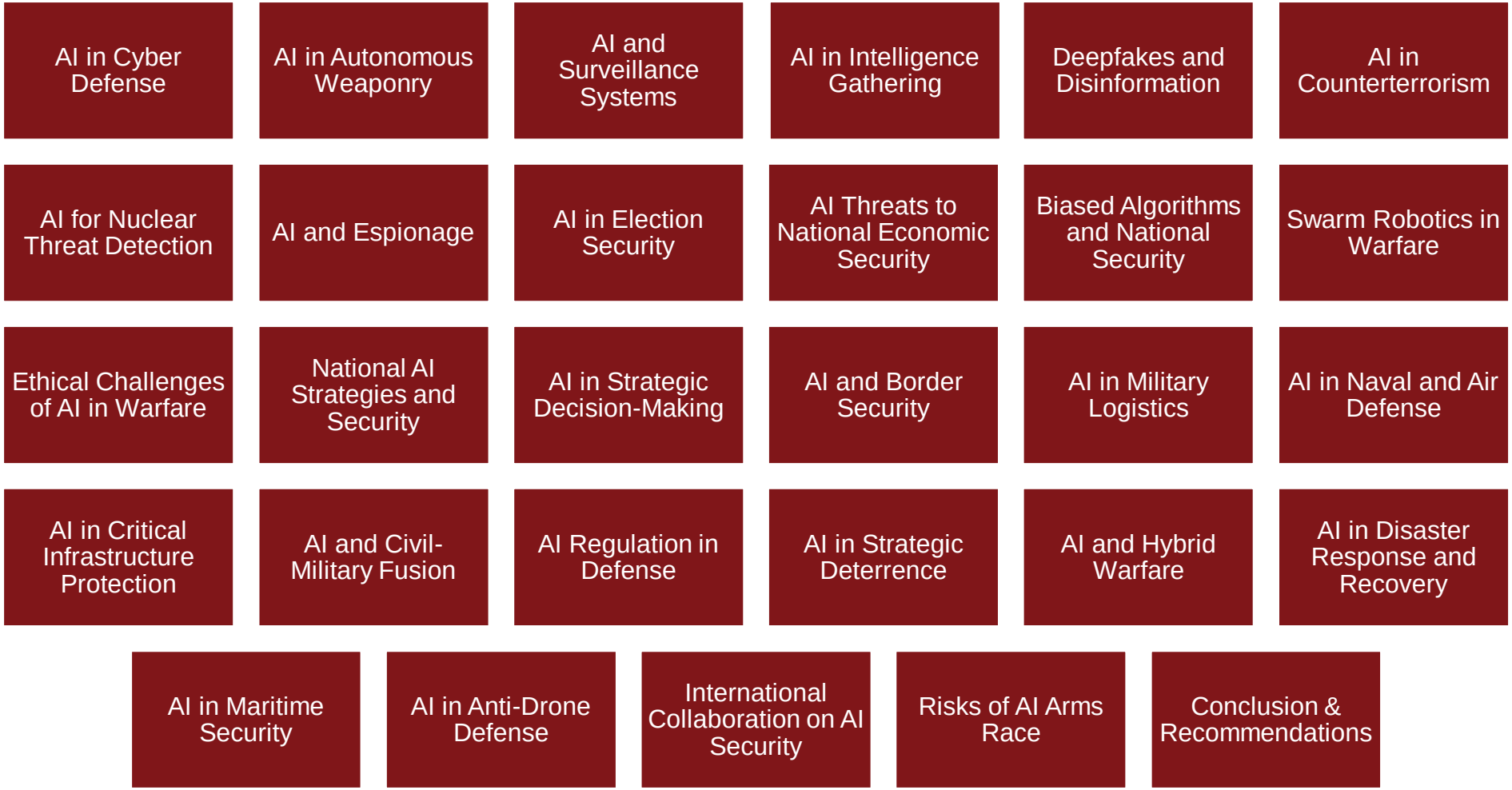
- Not all risks can be anticipated from the beginning due to the volume of data that AI can process, the speed of processing and the complexity of the algorithm
- AI impact may be wider and greater than with other software and technology solutions
- Generative AI must be created with necessary controls in place as it can be very difficult to see the warning signs when things move quickly

Legal and regulatory

- Industry laws and regulations may apply to AI use (e.g., pharmaceutical, telecom, financial).
- Privacy law implications; competition law; trade; tax.
- Breach of legal and regulatory risks can lead to sanctions, fines and orders to stop processing.
- Given the nature of AI to continue to learn and evolve, it can be difficult to anticipate what forms risks may take, particularly for new risks. Therefore, it is essential to apply AI principles and ethics rigorously to the development and testing of AI to mitigate these potential harms.
- Engage key stakeholders to understand potential harms.

MSECB

AI: Expanding Opportunities and Risks for National Security



MSECB

AI in Cyber Defense

AI technologies enhance cybersecurity by detecting threats in real-time, automating incident response, and identifying patterns across vast data sets. However, adversaries also use AI to conduct sophisticated attacks.

A May 2025 McKinsey analysis explains that AI is both a powerful shield and a potent weapon in cyber conflict. On the defensive side, AI enhances real-time threat detection, automates incident response, and applies predictive analytics. It can flag anomalies in network traffic, reverse-engineer malware, and predict vulnerabilities. Meanwhile, adversaries wield AI offensively—automating reconnaissance, launching adaptive attacks, generating deepfakes, and weaponizing the technology to compromise systems faster than humans can react. The report underscores a growing arms race in cyber capabilities, recommending better foundational security practices, AI explainability, public–private partnerships, and skilled workforce development

MSECB

AI in Autonomous Weaponry

- In brief:
- **Autonomous targeting**: All sources discuss AWS's ability to detect and engage without human control.
- **Safety & ethics**: They warn about unpredictable behavior, wrongful strikes, and civilian harm.
- **Accidental misuse**: The potential for unintended engagements is a recurring theme.
- **Escalation risk**: The speed and automation of AWS could lower conflict thresholds and provoke arms races.

- Autonomous weapons, powered by AI, can identify and engage targets without human intervention. This raises safety concerns and ethical dilemmas, including accidental engagements and escalation of conflicts.

MSECB

AI and Surveillance Systems

AI enables advanced surveillance technologies, including facial recognition and behavioral analytics. While effective for law enforcement, these tools also threaten civil liberties and privacy.

Artificial intelligence is making surveillance systems faster, more accurate, and capable of monitoring large populations in real time. It can analyze video feeds, recognize faces, detect unusual behavior, and predict potential threats using vast amounts of data. These advancements offer benefits like improved public safety and streamlined security operations. However, they also raise serious concerns about privacy, misuse, and lack of accountability, especially when deployed without clear oversight. Strong safeguards and transparent regulations are essential to ensure these technologies do not undermine civil liberties.

AI in Intelligence Gathering

- AI processes vast datasets from open-source intelligence (OSINT) to satellite imagery, enhancing decision-making. Yet, over-reliance on AI-generated intelligence can result in misinterpretation.

- Source: https://www.cnas.org/publications/reports/artificial-intelligence-and-national-security

MSECB

AI in Intelligence Gathering

AI processes vast datasets from open-source intelligence (OSINT) to satellite imagery, enhancing decision-making. Yet, over-reliance on AI-generated intelligence can result in misinterpretation.

Artificial intelligence is transforming national security by enabling faster data analysis, improving decision-making, and enhancing capabilities in areas like surveillance, logistics, and cyber defense. Machine learning systems can process vast and complex datasets to identify threats, optimize operations, and automate tasks that traditionally required human input. However, the integration of AI also introduces new challenges, such as ethical concerns, vulnerabilities to adversarial attacks, and the potential for strategic instability. Ensuring responsible development, clear oversight, and international cooperation is essential to maximize benefits while managing the associated risks.

Deepfakes and Disinformation

AI-generated deepfakes can create realistic fake videos, contributing to misinformation and political instability. Nation-states may weaponize deepfakes to influence elections or policy decisions.

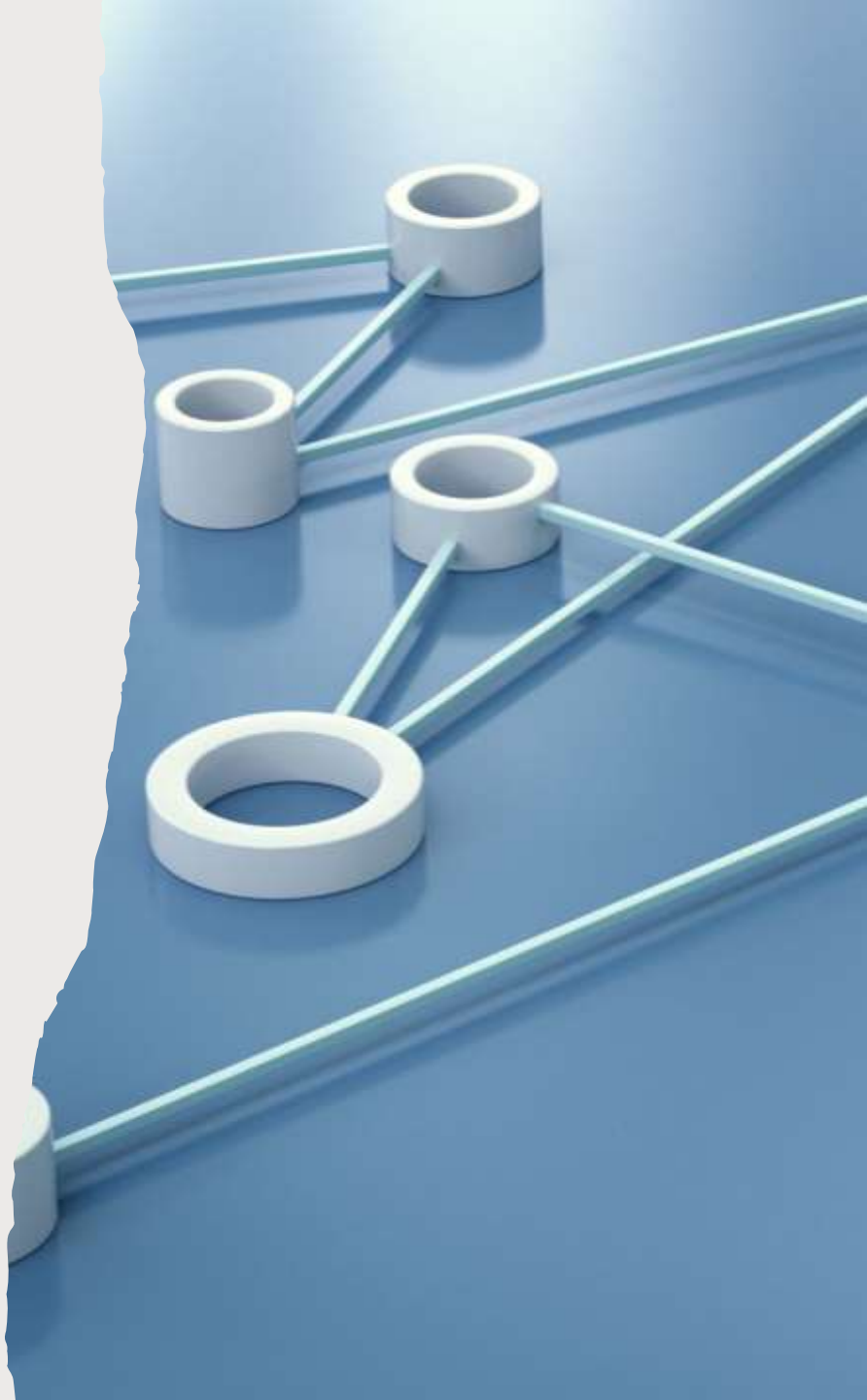
The BBC reported that Google has integrated generative AI into its core search engine through the **Search Generative Experience (SGE)**, enabling users to receive narrative, conversational responses to complex queries instead of just links to sources. These AI-powered summaries draw from multiple web pages to provide coherent and informed answers, improving user efficiency. However, early rollout revealed some notable inaccuracies—such as bizarre advice to eat glue or pizza with unusual toppings—prompting Google to refine the feature and restrict its use in health-related searches. As competition intensifies with Microsoft's AI-enhanced Bing, Google is accelerating its AI roadmap, including a broader rollout of AI-driven search features in 2025 .

MSECB

AI in Counterterrorism

AI tools analyze communications, behavior, and networks to detect and prevent terrorist activity. While effective, they risk profiling and violating privacy if not governed properly.

AI technologies are increasingly used to monitor communications, behavioral patterns, and social networks to identify and prevent potential terrorist threats. These tools can process vast amounts of data in real time, flagging suspicious activities and helping authorities respond more swiftly. However, without strict oversight and ethical guidelines, such systems risk unfairly targeting individuals based on biased algorithms or incomplete information. This raises serious concerns about profiling, misuse of personal data, and infringement on civil liberties. Responsible governance is essential to balance security needs with fundamental rights.



MSECB

AI in Counterterrorism (cont.)

Following 9/11, intelligence organizations rapidly incorporated AI and advanced analytics into counterterrorism operations. While machine learning can uncover hidden patterns in vast datasets—like communications, travel, and behavioral data—there's no substitute for human insight. Crucially, the article stresses the need for "human-in-the-loop" systems to prevent overreliance on opaque algorithms prone to bias, misclassification, or failure in adversarial environments. It highlights ethical and legal dilemmas, calling for rigorous oversight, data safeguards, and transparency to ensure predictive AI supports security without compromising civil liberties.

MSECB

AI in Counterterrorism (cont.)

The report explores how artificial intelligence is transforming counterterrorism by enhancing surveillance, data analysis, and threat detection capabilities. AI tools can process massive datasets to identify suspicious behavior, track networks, and uncover plots in real time, offering significant advantages to national security agencies. However, the piece also highlights serious risks, including misuse by extremist groups for propaganda or deepfakes, as well as the dangers of biased profiling, privacy violations, and overreliance on automated systems. It stresses the need for ethical frameworks, international cooperation, and strong regulatory oversight to ensure AI is used responsibly and effectively in combating terrorism.

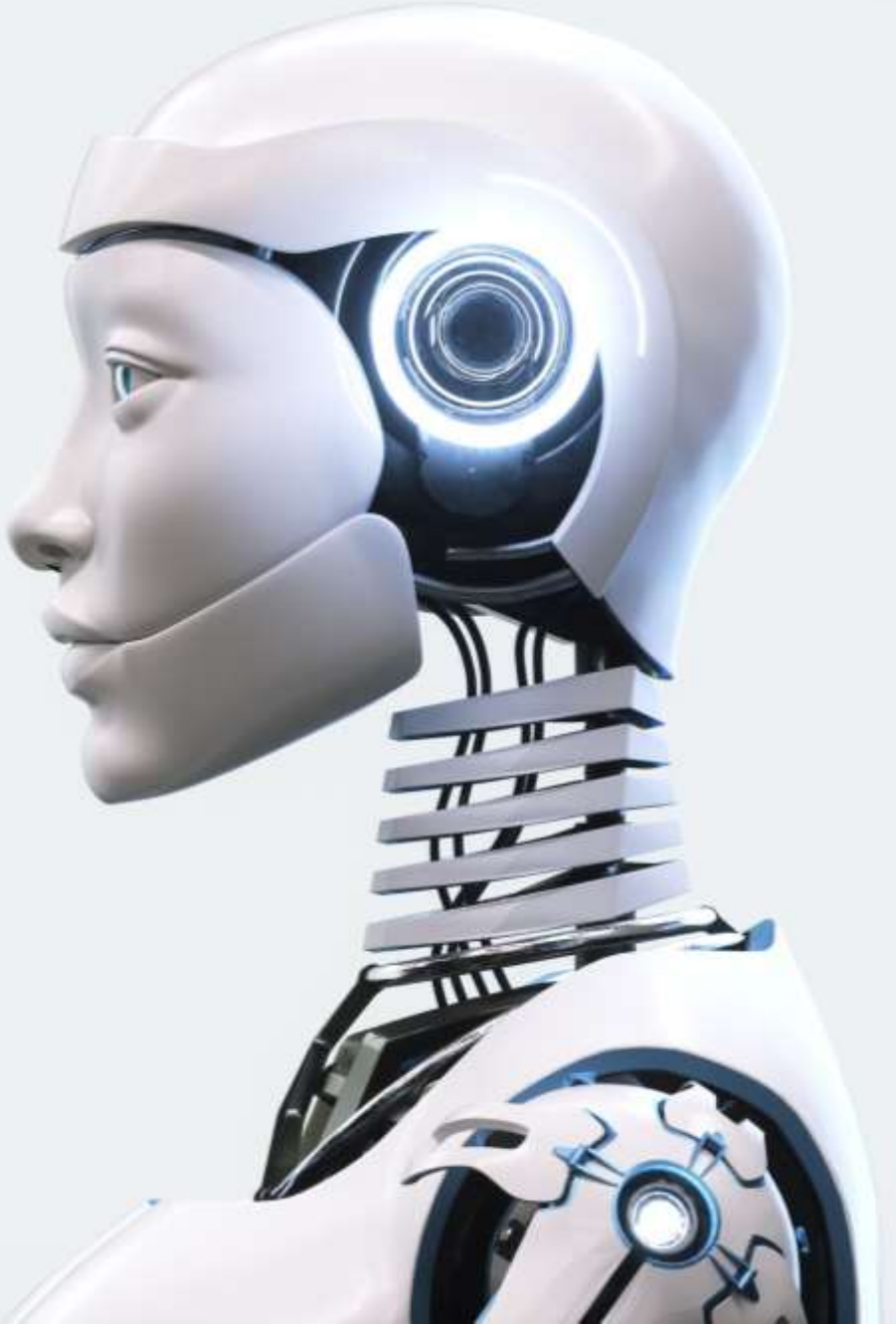
MSECB

AI in Election Security

AI defends electoral systems against interference but can also be used to manipulate voters through psychographic targeting and deepfakes.

The piece paints a chilling scenario where AI-generated deepfakes—showing fabricated voter fraud or ballot tampering—could erupt immediately after Election Day and rapidly go viral, overwhelming the ability of election officials to respond. Drawing from war-game exercises, the author highlights how adversaries now see greater value in sowing post-election chaos rather than altering votes directly. Election officials admit they're unprepared for fast-spreading, realistic fakes that may take weeks to debunk, by which point legitimacy and public trust could be severely harmed. The article calls for urgent measures including public awareness campaigns, adoption of content authentication tools, regulatory standards, and closer cooperation between officials and social platforms to safeguard electoral integrity before the vote.

MSECB



AI Threats to National Economic Security

AI affects labor markets, financial systems, and innovation pipelines. Economic AI shocks can destabilize national security.

Artificial intelligence poses growing risks to national economic security by accelerating job displacement, particularly in white-collar and service sectors. As AI systems automate tasks once considered safe from technological disruption, entire segments of the workforce may face instability, potentially widening economic inequality and reducing consumer confidence. This rapid shift can strain public institutions, weaken innovation pipelines, and create vulnerabilities within financial systems. Without proactive policy responses—such as investment in education, retraining, and stronger safety nets—nations may find their economic foundations eroded, which in turn can compromise broader national security.

MSECB

Shaping preferences and decisions: For example, platforms like YouTube or Netflix use AI to recommend content based on what you've watched before, guiding your behavior toward specific types of content.

YouTube's Anorexia Algorithm: How YouTube recommends harmful eating disorder videos to young girls

Posted on December 10, 2024 in Press releases

Share

RESEARCH ARTICLE | COMPUTER SCIENCES

Causally estimating the effect of YouTube's recommender system using counterfactual bots

Homa Hosseinmardi, Amir Ghasemian, Miguel Rivera-Lanas, +2, and Duncan J. Watts Authors Info & Affiliations

Edited by Christopher A. Bail, Duke University, Durham, NC; received August 8, 2023; accepted December 13, 2023, by Editorial Board Member Mark Granovetter

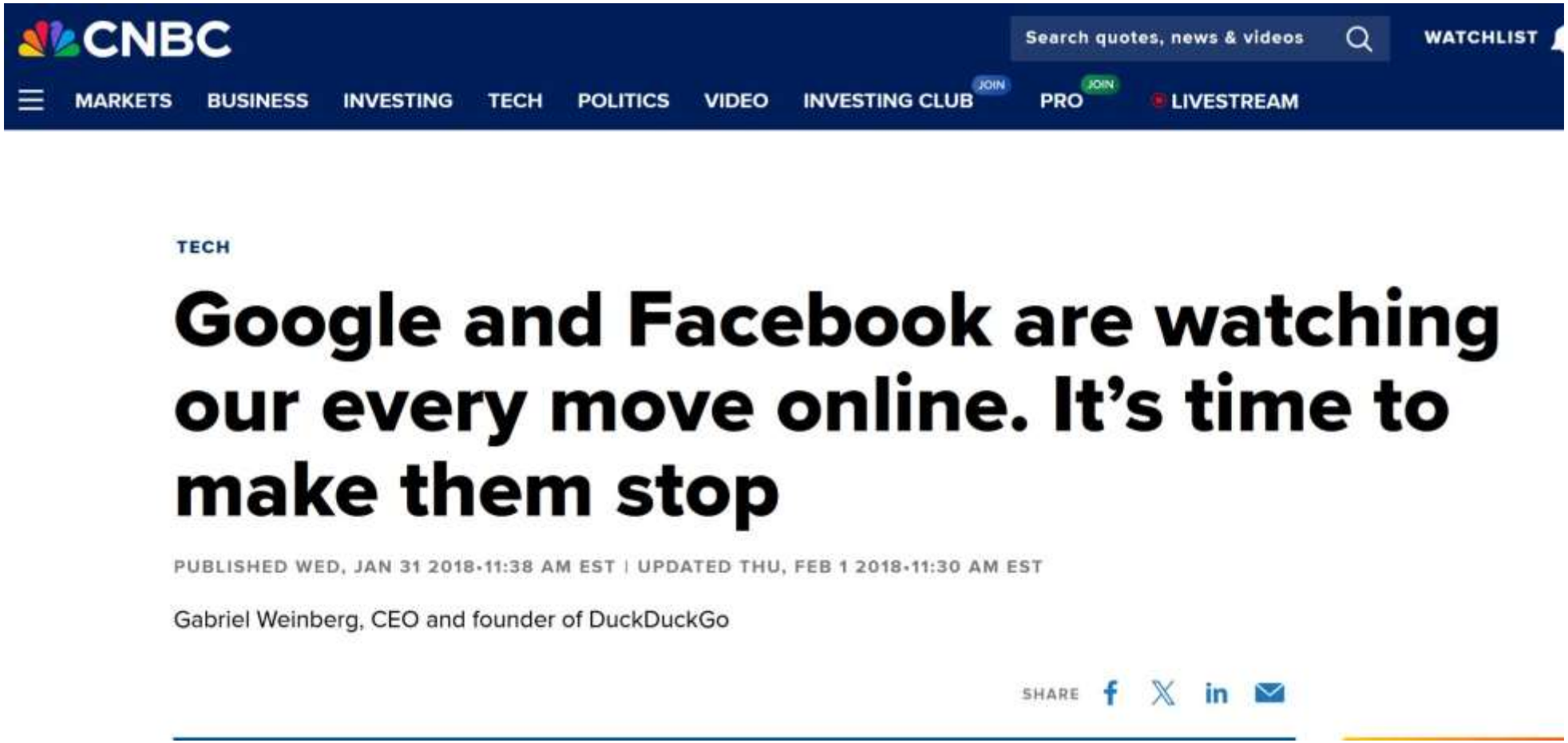
February 13, 2024 | 121 (8) e2313377121 | https://doi.org/10.1073/pnas.2313377121

MSECB

Reinforcing information bubbles: For instance, Facebook algorithms show you posts that align with your views, reducing your exposure to different perspectives — creating what's known as "echo chambers."

MSECB

Impact on privacy: A practical example is the collection of your location or activity data across apps, which can make you feel monitored and influence your daily behavior.



MSECB

Increasing digital addiction (especially among children and teenagers): Games or apps like TikTok are designed to capture young users' attention for long periods, increasing their attachment to screens.

MSECB

Impact on independent decision-making: When algorithms limit the options presented to you, they influence how you make choices — especially for teenagers who are still developing their reasoning skills.

powered by WiGen

Algorithmic Bias and Its Ethical Implications in Decision-Making

World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

WJARR

(RESEARCH ARTICLE)

Algorithmic bias in educational systems: Examining the impact of AI-driven decisi making in modern education

Obed Boateng * and Bright Boateng

Independent Researcher, USA.

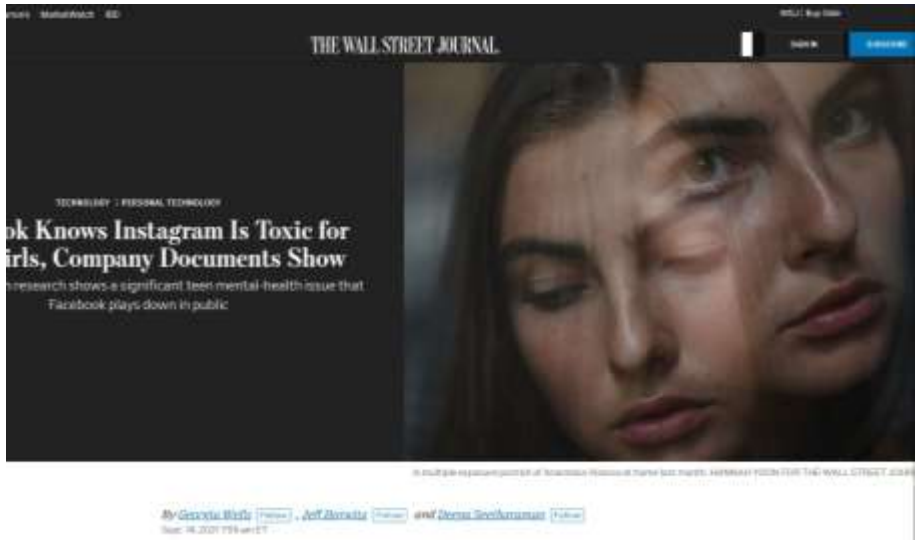
World Journal of Advanced Research and Reviews, 2025, 25(01), 2012-2017

Publication history: Received on 15 December 2024; revised on 25 January 2025; accepted on 28 January 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.1.0253

MSECB

Impact on independent decision-making: When algorithms limit the options presented to you, they influence how you make choices — especially for teenagers who are still developing their reasoning skills.



MSECB

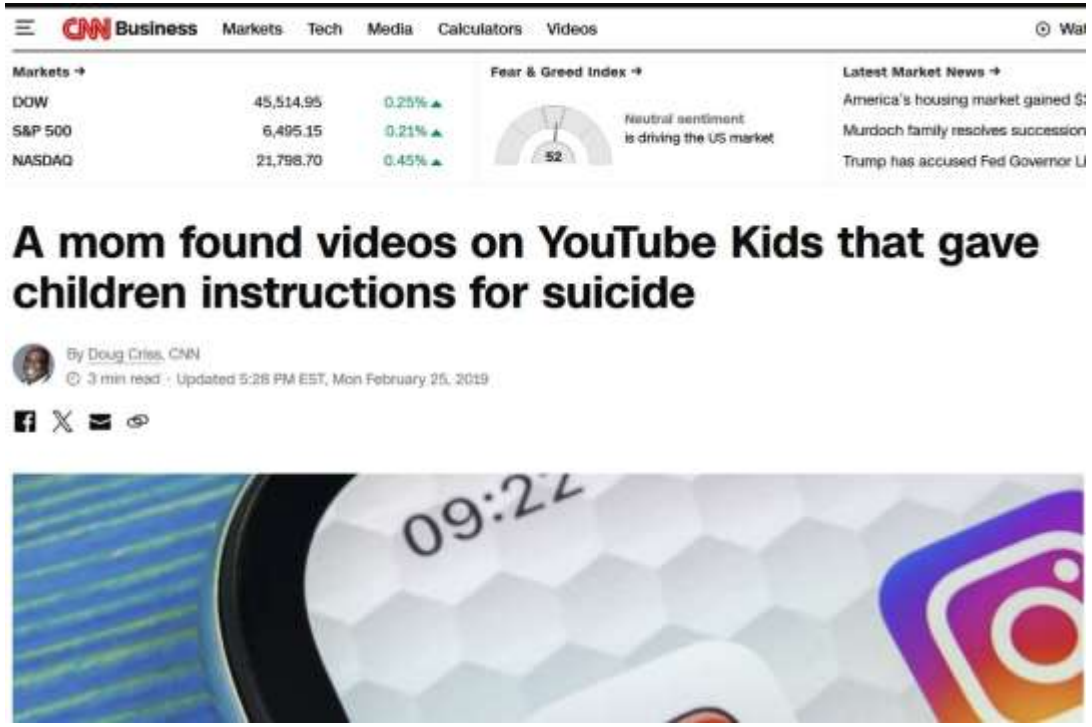
Shaping identity and social behavior: Platforms like Instagram may push teenagers to compare themselves to unrealistic beauty standards, affecting their self-image.

MSECB

Affecting social skills: Relying on digital communication (like chatting instead of meeting in person) may reduce teenagers' ability to interact effectively face-to-face.

MSECB

Greater exposure to inappropriate content: For example, children may encounter unsuitable videos on YouTube Kids due to inaccurate algorithmic recommendations.



Google says it will add new parental controls to its YouTube Kids app, after inappropriate videos were repeatedly discovered on the service.

MSECB

Impact on mental health: Constant interaction with social platforms that encourage social comparison can increase anxiety or depression among teenagers.

MSECB

Influence on consumer behavior and advertising: For instance, targeted ads on Instagram may encourage teenagers to make frequent or impulsive purchases.

Journal of Retailing and Consumer Services

Volume 59, March 2021, 102345

‘Instagram made Me buy it’: Generation Z impulse purchases in fashion industry

Elmira Djafarova [a], Tamar Bowes [b]

Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/j.jretconser.2020.102345

Get rights and content

Abstract

This paper investigates what types of Instagram marketing tools are the most effective in relation to Generation Z's impulse purchasing behaviour within fashion industry in the context of the United Kingdom. The research applies Stimulus-Organism-Response model to the context of Instagram. The findings of this qualitative study based on eight extensive focus groups conclude that there are significant gender differences in relation to impulse purchasing behaviour on Instagram. Instagram is vastly influential in encouraging impulse purchases amongst females, however, this was not the case for

Open Access Article

Instagram Mega-Influencers’ Effect on Generation Z’s Intention to Purchase: A Technology Acceptance Model and Source Credibility Model Perspective

by Rodney Duffett * and Ayabonga Mxunyelwa

Marketing Department, Faculty of Business and Management Sciences, Cape Peninsula University of Technology, Cape Town 8000, South Africa

* Author to whom correspondence should be addressed.

J. Theor. Appl. Electron. Commer. Res. **2025**, *20*(2), 94; https://doi.org/10.3390/jtaer20020094

Submission received: 20 February 2025 / Revised: 7 April 2025 / Accepted: 28 April 2025 / Published: 6 May 2025

Download Browse Figure Versions Notes

Q&A

Thank you for your attention!

Stay updated!

+1 (450) 328-1227

info@msecb.com

www.msecb.com