
From Human Intelligence Gathering and Social Engineering to Artificial Intelligence – An Impact on Society

Key Concepts

- Human Intelligence Gathering, Social Engineering and Artificial Intelligence.
- How We Started.
- Where We Are Going.
- What To Look Out For.
- Impact On Society - Brace for Impact.

Information Sharing Transition

- We have come from a society of privacy and keeping things to ourselves.
- To a society of information flow, sharing and giving.



Knowledge Explosion

- Information Sharing
 - Created a Knowledge Explosion.
 - Internet Use and Capability Grows Exponentially.



Human Intelligence Gathering

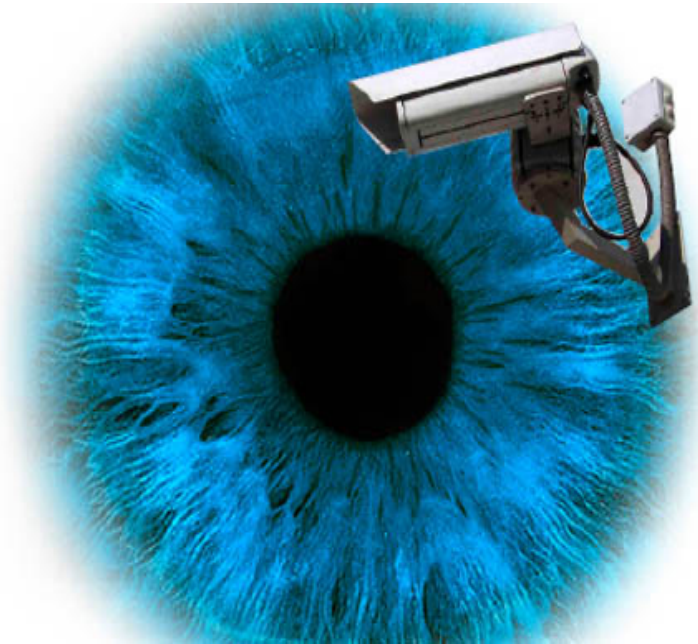
- What is it?
 - (HUMINT) Collection of data or information from people (humans) about any topic.
 - Collected Openly/Covertly.
- Human Intelligence Gathering
 - Automatically Leads to Social Engineering.

Social Engineering

- What is it?
 - Tricking or coercing people into revealing information or violating security practices.
 - Uses - Viruses, Trojan horses, Scareware, and Phishing all rely on trickery to be effective.
 - Rely on the human element.

Who is Watching You?

- Do you ever feel like someone is watching you? Well they are! Adversaries continually monitor web sites and personal activity to gather as much information on you as they can.



History - Jihadists Calls for Critical Information

- "Information on every U.S. naval unit - and only U.S. [units]! - should be quietly gathered [as follows:] [The vessel's] name, the missions it is assigned; its current location; the advantages of this naval unit; the number of U.S. troops on board, including if possible their ranks, and what state they are from, **their family situation, and where their family members (wife and children) live**; what kind of weapons they carry; the [vessel's] destination; the missions it has carried out; the way to monitor it around the clock; if its location is changed, define its movements and its route; **monitor every Web site used by the personnel on these ships**, and attempt to discover what is in these contacts."

Source: Philip Ewing, Staff writer on January 6, 2010 Navy Times

History - Lifestyle Spy

- Watches Subjects Movements
- Notes Associates
- Identifies Patterns



Who Else is Watching - Russia

Russia will ask permission on Monday to start flying surveillance planes equipped with high-powered digital cameras amid warnings from U.S. intelligence and military officials that such overflights help Moscow collect intelligence on the United States.

Russia and the United States are signatories to the Open Skies Treaty, which allows unarmed observation flights over the entire territory of all 34 member nations to foster transparency about military activity and help monitor arms control and other agreements. Senior intelligence and military officials, however, worry that Russia is taking advantage of technological advances to violate the spirit of the treaty.

Who Else is Watching - Drones

In a partnership with CNN, drone manufacturer [PrecisionHawk](#) and [BNSF Railroad](#), the [Federal Aviation Administration \(FAA\)](#) announced it will test-fly an undisclosed number of small drones for collecting news, according to a report by [Buzzfeed](#).

The move follows a drafting of [FAA rules governing commercial drone operations](#) across the country, which would require commercial drones to fly below altitudes of 500 feet and remain within the line of sight of the operator on the ground.

Despite these requirements, [the rules failed to mention concerns regarding privacy](#). And while a federal lawsuit, proposed laws, and voluntary guidelines are all attempting to enforce privacy standards for commercial drones, many privacy advocates feel as though it may be too late.

[Drones are getting smaller and more agile and many of them will soon feature cameras with facial recognition software, according to an April Congressional Research Service report on privacy threats from drones.](#)

[The FAA estimates that there will be up to 7,500 commercial drones in use by 2018, while a market analysis estimates that the industry will be worth \\$5 billion by 2019](#)

Source: <http://www.biometricupdate.com/201505/public-drones-equipped-with-facial-recognition-software-raise-privacy-concerns>

Drones – Facial Recognition



- Take pictures of you
 - Correlate those pictures with other databases
 - FB
 - Pinterest
 - Drivers License
 - Verify who you are!!!



Who Else is Watching - Drones

DARPA shows off 1.8-gigapixel surveillance drone, can spot a terrorist from 20,000 feet

By [Sebastian Anthony](#) on January 28, 2013 at 11:07 am

DARPA and the US Army have taken the wraps off **ARGUS-IS**, a 1.8-gigapixel video surveillance platform that can resolve details as small as six inches from an altitude of 20,000 feet (6km). ARGUS is by far the highest-resolution surveillance platform in the world, and probably the highest-resolution camera in the world, period.

ARGUS, which would be attached to some kind of unmanned UAV (such as the Predator) and flown at an altitude of around 20,000 feet, can observe an area of 25 square kilometers (10sqmi) at any one time. If ARGUS was hovering over New York City, it could observe half of Manhattan. Two ARGUS-equipped drones, and the US could keep an eye on the entirety of Manhattan, 24/7.

Source: <http://www.extremetech.com/extreme/146909-darpa-shows-off-1-8-gigapixel-surveillance-drone-can-spot-a-terrorist-from-20000-feet>

Scraping

- FOR LAW ENFORCEMENT USE ONLY - Clearview AI
- Created software that scraped Billions of Faces off social media sites.
 - Matched faces with names.
 - Could identify people with only a small portion of their face visible.
 - Social Media sites sent legal cease and desist order
 - Too late the software is out, and people are being tracked.

Who Else is Watching - China

How China's Spies Can Watch You At Your Desk

60 Minutes reports on **how the Chinese government steals trade secrets from American business people-and why CEOs in the U.S. keep it quiet.**

- This week on 60 Minutes, Lesley Stahl explores the **devastating impact of Chinese corporate spying and intellectual property theft.** The story reports that U.S. **companies have already lost hundreds of billions of dollars** and more than two million jobs to what's been called "the great brain robbery" of America.
- In some cases, **they send a fake email to a U.S. worker that looks as if it comes from a colleague.** If the worker clicks on the attachment, the **Chinese hacker can not only steal documents, but also activate the computer's camera to watch the worker and listen in on conversations.** The goal of such spying, the story explains, is for China to advance its own industries without putting in the research or funding required.
- While American **CEOs** know they're being spied on, they are often **reluctant to report it for fear of losing their foothold in China,** the world's second largest economy.

- Source: <http://www.cbsnews.com/news/60-minutes-overtime-how-chinas-spies-can-watch-you-at-your-desk/>

China – Intellectual Property

- To do business with China you must surrender your intellectual property.

Intellectual Property
???????

Mission: The National Security Agency leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances.



The Information Assurance mission confronts the formidable challenge of preventing foreign adversaries from gaining access to sensitive or classified national security information. The Signals Intelligence mission collects, processes, and disseminates intelligence information from foreign signals for intelligence and counterintelligence purposes and to support military operations. This Agency also enables Network Warfare operations to defeat terrorists and their organizations at home and abroad, consistent with U.S. laws and the protection of privacy and civil liberties.

Remember ME? – Insider Threat



What Did He Do?

- In date, Snowden contacted Snowden first made contact with Glenn Greenwald, a journalist working at *The Guardian*, in late 2012
- Snowden then contacted documentary filmmaker Laura Poitras in January
- Greenwald began working with Snowden in either February^[96] or April 2013, after Poitras asked Greenwald to meet her in New York City, at which point Snowden began providing documents to them.^[90] Barton Gellman, writing for *The Washington Post*, says his first "direct contact" was on May 16, 2013.
- Ultimately provided information to Wiki Leaks and Julian Assange
- Leaked
 - Australian – 15,000
 - British – 58,000
 - United States – 1.7 million

Chelsea Manning

- U.S Army Intelligence Analysts.
- Leaked Classified Military Operations Documents to Media.
- Sentenced to 35 years in prison reduced to 7.



The Virtual World

- It is a real place, or the stuff movies are made of?



Current Conflicts

- International events are playing out in the Virtual World and the Physical World.
 - Russian Invades Ukraine.

Current Conflicts

- Director of National Intelligence - Avril Haynes stated weeks before the invasion of Ukraine, that Chevron and other companies were virtually attacked by Russia in an attempted to shut them down.
 - Russia has multi-phase plans to destabilize the US power industry.
 - Targeting the US financial sector.
 - Due to the blurred lines between the virtual world and the physical world - Cyber attack could trigger NATO Article 5.

Current Conflicts

- Cybersecurity and Infrastructure Security Agency and FBI:
 - Top pharmaceutical companies were targeted by Russian hackers.
 - Done by cyber training units inside of Russia.
 - Russia is deploying ransom ware across all agencies.

Russia Is Not Alone

- Collaboration Russia-China
 - Nicolas Chaillan, U.S. Air Force former Chief Software Officer.
 - U.S is at kindergarten level relating to critical infrastructure compared to Russian-China alliance and cyber offensive capabilities.
 - Russian-China cyber collaboration will be devastating to the US.
- Conversely, the International Institute for Strategic Studies placed the US in its top tier of cyber powers and Russia and China in tier two.

China a Threat?

- CIA director says China is the greatest challenge to the US.
- 100-year plan to destroy the US.
- New Craze in US is Tik-Tok – Sen. Josh Hawley – Owned by Chinese businessman and is ultimately controlled by Beijing China.

Your Best Friend is Not Your Friend



What Apps Are You Installing?

Your Best Friend is Not Your Friend



- Take pictures
- Turn camera on and off
- Listen to Phone Calls

Recent Threats

- Pegasus Software
 - Developed by Israeli NSO Group.
 - Made to compromise phones.
 - Effected Heads of State, Reporters.
 - Turns a phone into a surveillance device.
 - Access Camera and Microphone.
- Log4j
 - Log activities of consumer facing products.
 - Can be used to capture and retrieve intellectual property.
- Sen. Wyden from Oregon – SS7 International telecommunications protocol can be compromised and allow foreign actors to gain unauthorized access to our networks and intercept calls and texts.

Recent Threats

- Apple Air Tag attached to a family at Disney.
 - Very similar to micro-dots of the past.
 - Air tags can be detected with android apps and other tools.



Pictures are Deadly – Proud Papa



Artificial Intelligence Explosion

- What is it?
 - Human like intelligence demonstrated by machines.
 - NOT predetermined coded routines.
- Intelligence determinations derived through processes conducted by computer information systems.
- Results In
 - Rapid Technological Advancement.
 - Many Benefits and Positive Effects.



Types of Artificial Intelligence



- Reactive Machines
 - Operates on set of rules and reacts to stimuli.
 - IBM Deep Blue Chess Championship.
- Limited Memory
 - Stores previous data and uses it to make future predictions.
- Theory of Mind
 - Understands emotions, beliefs, thinking, and needs of individual humans and reacts in real time.
- Self Awareness
 - Becomes self aware and forms its own identity.

Dangers of Artificial Intelligence

- Jobs
 - Job Displacement – Job Loss.
 - Current jobs being replaced by AI – Dark Factories.
- Bias Decision Making
 - AI can inherit biases from its originators.
- Ethical Concerns
 - Can ethics be programmed into AI and whose ethics are being used.
 - Organizations and guidelines for ethical development.
- Privacy Concerns – Collects a tremendous amount of PII at an accelerated rate.
- Superintelligent AI – Surpass human process capabilities – Lose control.
- AI Powered Networks and Weapons – Lose control.

Artificial Intelligence Oversight

- AI System Accountability – Very few initiatives currently in place or perfected.
 - Companies have published their ethical principals.
 - Companies do audit AI algorithms.
 - Identify bias training datasets.
- Explainable AI – AI models that explain their decision-making process and how they arrive at their conclusions.
- Accountability in AI.
 - Algorithmic Auditing.
- AI Impact Assessment.
- AI Certification and Standardization.
- Regulatory Initiatives.
 - Requirements for transparency, data protection and compliance.

Artificial Intelligence in Human Intelligence Gathering

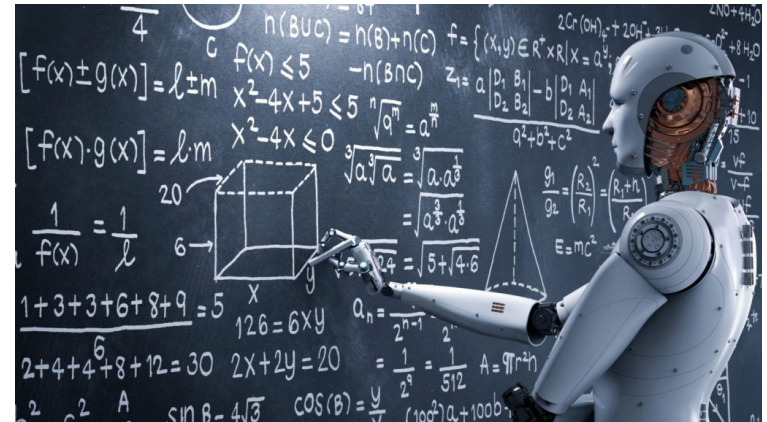
- Data Analysis and Pattern Recognition
 - Social Media.
 - Data Interception.
 - Identify Patterns Trends Anomalies.
- Sentiment Analysis
 - Gauge public opinion.
 - Used by foreign governments.
 - Collects large scale Information.
- Social Network Analysis
 - Analyze and identify various individuals, connections and relationships.
 - Used to map social networks to identify weaknesses and vulnerabilities.
- Anomaly Detection
 - Detect change in data patterns to identify vulnerabilities. Identify potential security risks.
- Image and Video Analysis
 - Track individuals' movement and identify patterns of behavior.
 - Predictive Analysis.

Artificial Intelligence In Social Engineering

- Spear Phishing
 - Automated - Review social/news media to create personalized attacks on specific individuals.
- Voice Impersonation
 - AI can imitate a person's voice and voice characteristics.
- Chatbots In Online Communities
 - Imitate real people and gather information for another attack.
- Deepfake Videos
 - Create lifelike video producing social influencing messages.
- Predict Behavior Patterns
 - Analyze data sets to predict patterns to influence social/political groups.
- Absolutely Convincing
 - Analyze Phishing Detecting mechanisms criteria and produce a product that evades identification.

Artificial Intelligence In Education Is Inevitable

- "AI in education is as inevitable as the internet or a search engine, which also people were skeptical about in the beginning," said Julia Dixon, a former tutor who created ES.AI, a generative AI tool for college applications. "Students who never use AI and those kinds of resources that can really up-level the work that they're doing are going to be at a disadvantage."



Source: <https://www.foxbusiness.com/technology/education-ai-inevitable-students-use-disadvantage-ai-founder>

Artificial Intelligence - Benefits

- AI Is Beneficial to Students
 - Brainstorming
 - Introducing New Concepts
 - Develop Outlines For Essays
 - Grade or Evaluate Student Assignments
 - Act As A Tutor
- **????Question Everything????**

Artificial Intelligence In Education – The Downside

- Currently students are turning in papers/assignments written entirely by AI.
- Losing deep/qualitative research skills.
- Losing creative baseline thinking and capability.
- Losing original development skills.
- Depending on technology.
- Student/Teacher interaction reduces.
- AI does not support individualized learning styles – It is very generic.
- Problem solving skills diminish.
- Student's reliance on AI reduces actual learning and ill preparedness when it comes to stand alone assessments.

Artificial Intelligence Impact on Society

- We Have Created a Virtual World.
 - Unquenchable Thirst for Knowledge.
 - Developed and Mastered Intelligence Gathering.
 - Use Intelligence for Global Domination.
 - Introduced and Continually Advance Artificial Intelligence.
 - Positioned Future Technological Experts to Be Reliant on Artificial Intelligence.
 - Placed Technology at the Forefront Civilization Advancement.
- Where do we go from here?