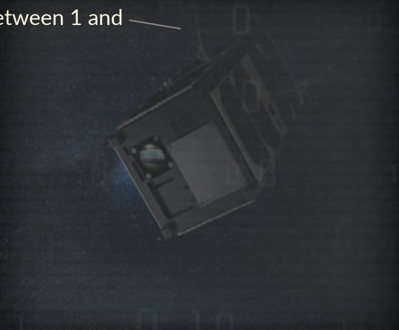
SPYCRAFT

SPYING IN THE 21ST CENTURY

BIG MEDIA

SPYCRAFT

OVERVIEW



NANO SATELLITES - The term “nanosatellite” or “nanosat” is usually applied to the name of an artificial satellite with a wet mass between 1 and 10 kg (2.2–22 lb).

DEEPFAKES - synthetic media in which a person in an existing image or video is replaced with someone else’s likeness.

METAVERSE - Virtual environments will supercharge disinformation campaigns, espionage and surveillance.

The secret collection of intelligence is said to be the second oldest profession. Following global success, Spycraft returns for another season. This time focusing on a new era of espionage. The days of sending spies wearing fake mustaches behind enemy lines to break into an office and take pictures of secret documents with their bowtie are over. The game has changed. Data is in the clouds and nuclear weapons are out of style. Everything is high tech. The new arms race is information based whether its state vs state or the state vs its own citizens.

EPISODE 1

Influence Operations - Weaponizing Social Media

FEATURED TECH:

- Social Media Bots
- Deep Fakes
- “Useful Idiots”
- Platform Algorithms

SYNOPSIS:

A virus doesn’t destroy you head on, it brings you down from the inside, turning your own cells into enemies. Fake news is not an accident that stems from a lack of fact checking, it’s a state on state strategy invented to slowly and methodically poison its enemies. In 2016, two Russian Facebook pages organized dueling rallies in front of an Islamic Center in Houston, Texas. Interactions between the two groups escalated into confrontations and verbal attacks. In the same year, Russian-sponsored articles circulated the internet making allegations a pizza parlor in Washington was harboring children as sex slaves as part of a child-abuse ring led by Hillary Clinton. This led to a man armed with an AR-15 shooting up the restaurant. This episode takes a look at the recipe behind fake news and the missions that used it . From adversaries using social media bots across the world to political rivalries using deep fakes to swing elections, it’s all part of the latest advances in spycraft.

EPISODE 2

THE KILL CHAIN

FEATURED TECH:

- Computerized Sharpshooter
- Remote Control Machine Gun
- Predator Drones
- Killer Robots

SYNOPSIS:

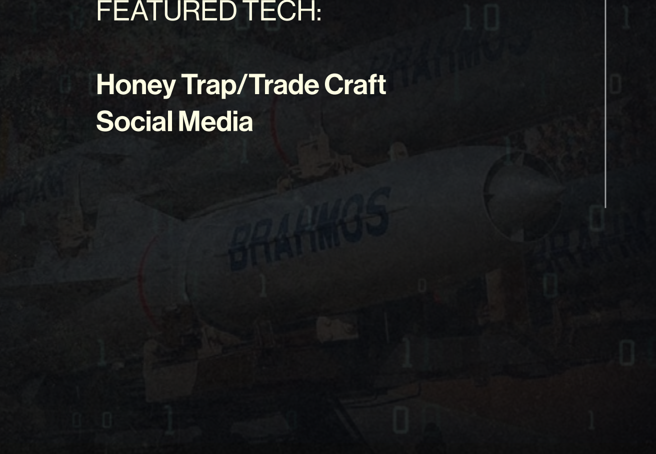
The Mossad assassination of the father of Iran's nuclear program in 2021 was conducted entirely through autonomous systems taking remote targeted killing to a new level when robots armed with weapons shot up his caravan. Killer robots can locate, select and attack using facial recognition systems to profile a target. The Cold War marked an arms race of nuclear weapons. The new arms race is cheaper and easier to build than a nuclear warhead. In 2018, Venezuelan President Nicolas Maduro survived an assasination attempt. While speaking at a military event, two drones loaded with explosives went off near the president's stand injuring seven soldiers. According to a March report from the U.N. Panel of Experts on Libya, lethal autonomous aircraft may have "hunted down and remotely engaged" soldiers and convoys fighting for Libyan general Khalifa Haftar. It's not clear who exactly deployed these killer robots, though remnants of one such machine found in Libya came from the Kargu-2 drone, which is made by Turkish military contractor STM. This episode highlights the latest systems used by countries, militaries and rogue actors to remove the human element from the Kill Chain in a new era of unmanned weapons.

EPISODE 3

Virtual Sexpionage

FEATURED TECH:

Honey Trap/Trade Craft
Social Media



SYNOPSIS:

For as long as espionage existed, there have been spies willing to use sex as a weapon to extract national secrets. Throughout history and up until the virtual age, countries like the UK and Russia heavily invested in training men and women on how to conduct these types of operations. Today, it's a different ballgame. In 2018, a Brahmos engineer was arrested for espionage, handing over information related to India and Russia's joint-venture AeroSpace manufacturers supersonic cruise missile, believed to be the fastest in its class and which can be fired from land, air and sea. What made him do it? A Virtual Honey Trap. The engineer was targeted by Pakistani agents posing as fake women on the web offering him sexual favors. He's not the only one. This episode takes us through a series of modern day honey trap targets from Israeli spies revealing nuclear secrets to a Pentagon linguist handing over a list of U.S. spies to her Hezbollah-linked handler.

EPISODE 4

Cyber CounterIntelligence & Crypto Dead Drops

FEATURED TECH:

- NFT/CryptoArt
- Cryptocurrency
- Blockchain

SYNOPSIS:

In early 2016, Russian intelligence officers obtained a new pool of the virtual currency Bitcoin. The Russian spies used some of the Bitcoins to pay for the registration of a website, dcleaks.com, where they would later post emails that had been stolen from Hillary Clinton's presidential campaign. When the operatives needed a computer server to host the dcleaks site, they paid for that with Bitcoins as well. In August of 2020 the United States government seized millions of dollars in over 300 cryptocurrency accounts linked to Hamas, Al Qaeda & ISIS. ISIS went as far as selling fake COVID-19 protective gear in an elaborate scheme that demonstrates how terrorist groups have adapted to the cyber age. From storing wealth in assets like NFT/Crypto Art to tracing money through a blockchain, this episode reveals an entirely new era of espionage and counter espionage in the cyber age where a briefcase full of cash is completely outdated.

EPISODE 5

Disguises & Botched Cover Ups

FEATURED TECH:

Five Second Mask
Ghillie Suit
Social Media

SYNOPSIS:

On a covert mission targeting a top Al Qaeda terrorist leader, US Navy SEAL Clint Emerson used a full-face latex mask to throw off surveillance so he could move freely in dangerous territory. It's called a "five second mask" because a user should be able to put it on in less than five seconds. During his time in Afghanistan, Malcom Nance wore a Ghillie Suit, also known as an invisibility cloak, to stay hidden in plain sight. From old-school Cold War disguise kits containing fake mustaches and wigs to modern day social media accounts and fake charity organizations, this episode takes a look at the evolution of disguises and botched cover ups.

EPISODE 6

Feed the Machine

FEATURED TECH:

- HIK Vision Cameras
- China's Police Facial Recognition Glasses
- Eyecool Biological Recognition Technology
- China's Police Cloud

SYNOPSIS:

In the race to build the ultimate spycraft, the quantum computer, China spies on and has imprisoned their own citizens. Certain communities are forced to hand over biometric data like blood, voice samples and DNA. This episode reveals China's social credit system and the spycraft they use on their own people. It also reveals China's successful attempts at collecting data on other countries by selling them new tech as well as apps. Chinese companies, many of which are state-owned, all of which are legally obliged to cooperate with the Chinese Communist Party on intelligence matters, have built at least 186 government buildings in Africa, including presidential residences, ministries of foreign affairs, and parliament buildings. Huawei has built more than 70 percent of the continent's 4G networks and at least fourteen intra-governmental ICT networks, including a data center in Zambia that houses the entirety of the government. The viewers will think twice before dancing on TikTok and realize accepting cookies from websites is the least of their problems.

SPYCRAFT

SPYING IN THE 21ST CENTURY

BIG MEDIA