



**TOP SECRET**

**Contains codeword material**



# What is Espionage?


**Espionage, spying, or intelligence gathering is the act of obtaining secret or confidential information (intelligence)**



**A person who commits espionage is called an espionage agent or spy**



**Any individual in the service of a government, company, criminal organization, can commit espionage**



**However, the term tends to be associated with state spying on potential or actual enemies for military purposes**

# How can espionage be carried out?

One way to gather data and information about a targeted organization is by infiltration



Spies can then return information such as the size and strength of enemy forces



They can also find dissidents within the organization and influence them to provide further information or to defect



In times of crisis, spies steal technology and sabotage the enemy in various ways



Counterintelligence is the practice of thwarting enemy espionage and intelligence-gathering

# Some Quotes

All warfare is based on deception. There is no place where espionage is not used. Offer the enemy bait to lure him

Sun Tzu

Once you've lived the inside-out world of espionage, you never shed it. It's a mentality, a double standard of existence

John le Carre

Generally speaking, espionage offers each spy an opportunity to go crazy in a way he finds irresistible

Kurt Vonnegut

The more we know about each other the safer we all are

William Colby

(said to Leonid Brezhnev)

# The history of espionage

Espionage has been recognized as important in military affairs since ancient times

Knowledge has always been power rulers needed to find out what enemies are

doing

thinking

planning

Even in earliest times, military operations required a scouting system

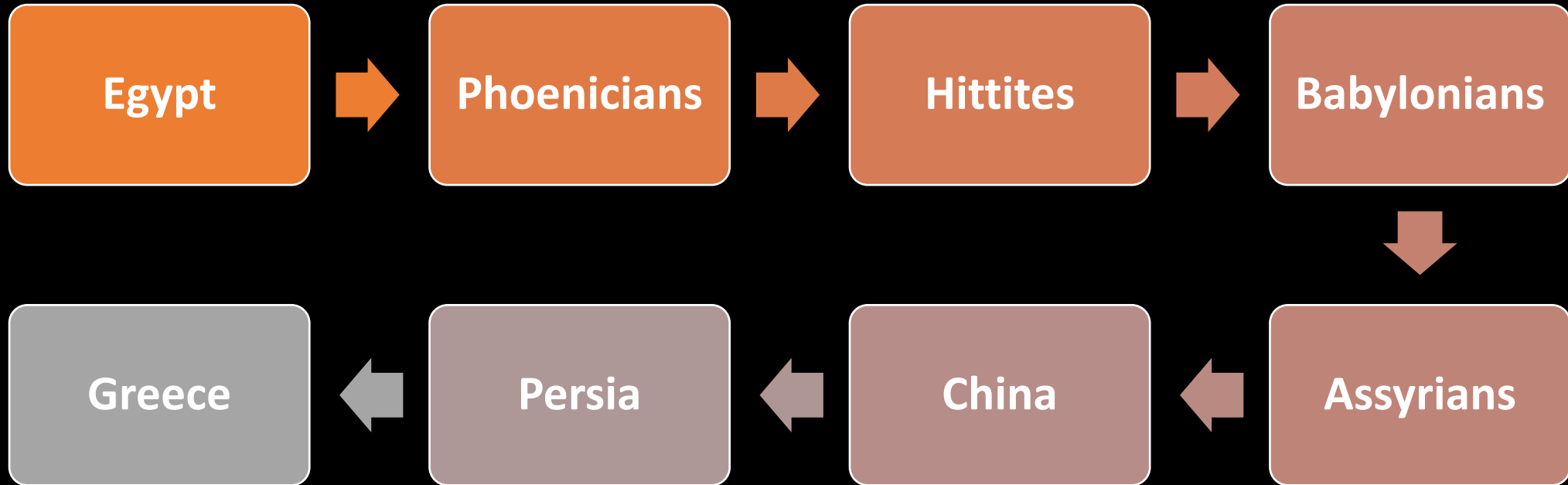
Military commanders taking their armies into unknown regions needed knowledge of

geographic conditions

the number and kinds of  
inhabitants in the land

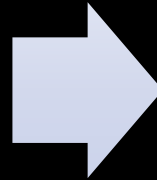
the strategic possibilities available  
to them

# The history of espionage - early examples include:

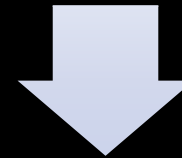


# The history of espionage

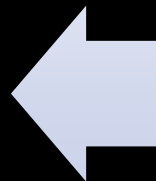
The Ancient Egyptians coined a new word for a new breed of public servant – “the eyes of the Pharaoh”



The Persian King Cyrus the Great (c. 590-530 BCE) called spies his many “eyes and ears”



*“It is only the enlightened ruler and the wise general who will use the highest intelligence of the army for the purposes of spying, and thereby they achieve great results.”*



The ancient Chinese military theorist General Sun Tzu (c. 554-496 BCE) devoted a chapter of his seminal “The Art of War” to the role of the spy.



# The history of espionage

The Ancient Greeks and Romans made extensive use of espionage, although the Romans took a long time to appreciate the importance of the spy

Nevertheless, having started, they made up for lost time by coining the name by which we now refer to the role of a secret agent

The Latin *spicere* (to look on) evolved into “spy” whilst the term “agent” is equally Latin – *agentes in rebus* or “agents in public mission”

The majority of medieval spies were priests and monks – able to read and write in a number of languages and spread in a network throughout Europe

The occupation underwent a wave of professionalization during the 15th century, with trained agents replacing the travelling merchants and soldiers previously used to gather information

# Elizabethan Intelligence Network

The counsellors of the Queen Elizabeth I (1533-1603) established the first dedicated intelligence network, led by Sir Francis Walsingham



He was a crucial figure in Elizabethan times, running the Secret Service as well as serving as Secretary of State during times of international conflict, including the Spanish Armada



In 1568 he began overseeing intelligence gathering operations designed to foil plots to overthrow the queen. He soon amassed a large network of spies, and created a professional secret service



He is best known for his role in securing the grim fate of Mary Queen of Scots, showing his loyalty to his queen as well as his sense of public duty in the face of external threats



Sir Francis Walsingham's trusted network of spies used invisible ink, as well as a special technique to open and reseal letters in order to keep abreast of plots



# Modern Times

The advent of new communication technologies such as the telegraph, telephone and photography in the 19th century changed the face of spying

Not only was it possible to collect information in new and ever-more covert methods; it could be communicated across large distances in real time

Later, human agents became ever-less important, to be replaced by machines

The intelligence organizations of World War Two played a decisive role in influencing the military course of the war

The British code breakers of Bletchley Park encoded the Enigma machine and could read Axis signal traffic and provide information vital to the war effort



# Cold War

The Cold War (1947-1989) was conducted to a greater extent than ever before as a war of espionage

The intelligence services were used both to gauge the strength of enemy forces and shore up various political systems

The collapse of the Warsaw Pact in the 1990s heralded a further paradigm change for the world's intelligence agencies

They are now forced to deal with industrial espionage and since 2001, the threat posed by international terrorism

Given the sheer scale of the internet and the vast volume of its data traffic, this poses a considerable challenge to the activities of today's spies

# What information are spies looking for?

Intelligence agencies are directed by their governments to focus their attention on specific priorities

State agencies, the military and companies working on sensitive technologies are prime targets for foreign espionage

Intelligence services working against the UK tend to focus on gaining a number of different types of secret information

# Military secrets

These will include

technical  
information  
about  
weapons

details of  
where troops  
are located

information on  
defences

This can be  
especially useful to  
an enemy country  
in wartime

It can help an  
enemy to find

weak points

or launch  
surprise  
attacks

It can also be  
useful to terrorists

it can help  
them to pick  
out targets

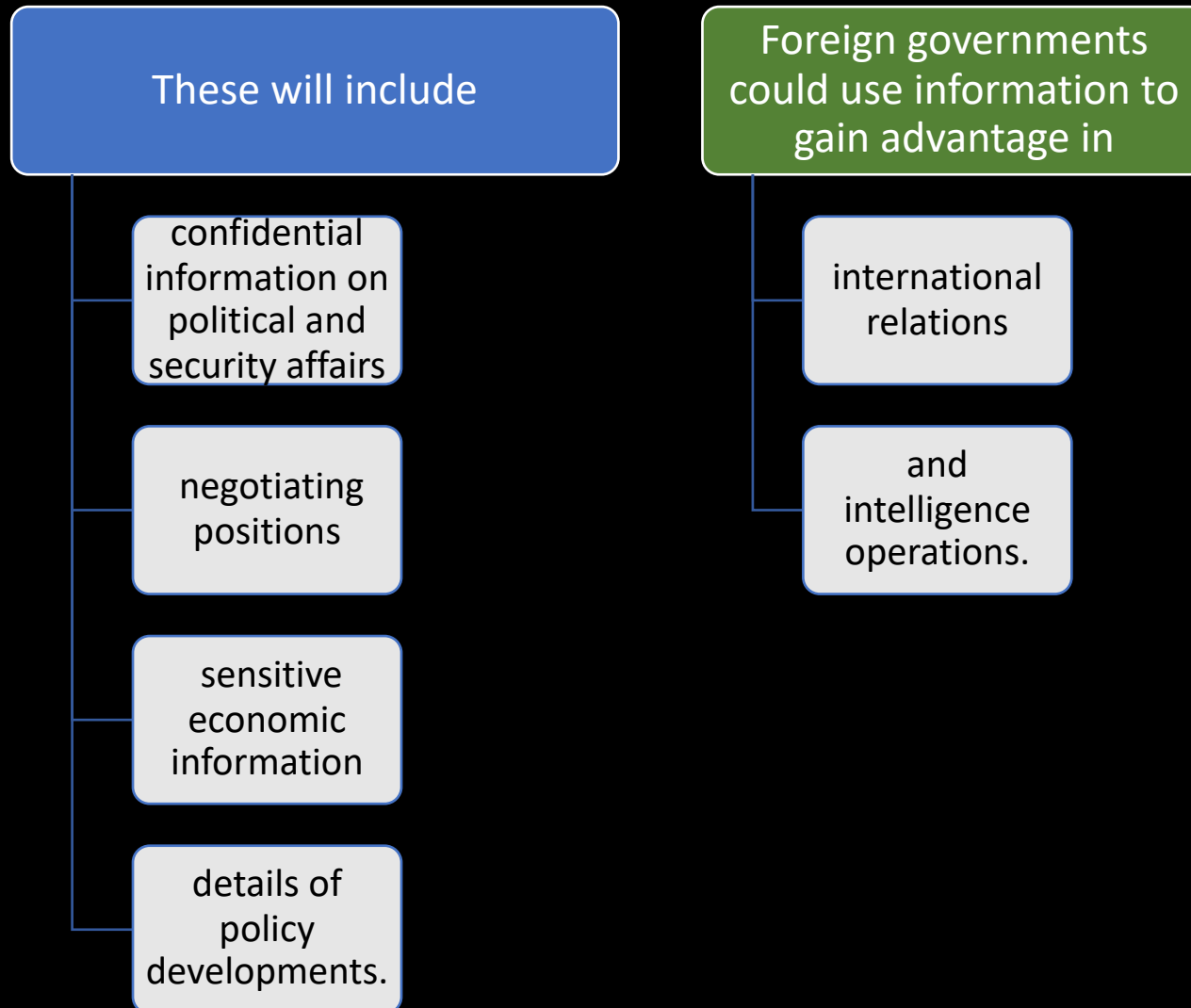
and weak  
points

# Industrial secrets

---

These will include  
information on  
companies' products and  
plans

# Political secrets





# How is espionage conducted?

Spies working for states fall into two categories:

intelligence officers and agents.

# Intelligence officers

Intelligence officers are members of intelligence services

They will be highly trained in espionage techniques and the use of agents.

They may operate openly, declaring themselves as representatives of foreign intelligence services

or covertly under the cover of other official positions such as diplomatic staff or trade delegates.

Some may operate under non-official cover to conceal that they work for an intelligence service


posing as a business person, student or journalist for example

In some cases they may operate in "deep cover" under false names and nationalities


Such spies are dubbed "illegals" because they operate without diplomatic immunity

# Agents

In the UK, an agent, more formally known as a "covert human intelligence source", is someone who secretly provides information to an intelligence officer



They will probably not be a professional "spy" but may have some basic instruction in espionage methods



An agent may be motivated by a wide variety of personal or ideological factors

# How intelligence officers and agents operate

Intelligence officers seek to gather covert intelligence directly and to recruit agents to obtain intelligence on their behalf

The methods used by intelligence officers vary widely and are often limited only by their ingenuity

They will often take advantage of the latest technology, using it to eavesdrop, tap telephone calls and communicate secretly.

However, the human relationship between intelligence officers and their agents remains a key element of espionage.

Foreign intelligence services typically seek to establish networks of agents whom they can use over a sustained period of time, so that they can obtain a reliable flow of information.

Agents operate by exploiting trusted relationships and positions to obtain sensitive information.

They may also look for vulnerabilities among those handling secrets.

They may be aware of flaws in their organisation's security that they can exploit.

# Cyber espionage

Espionage activity is also carried out in cyberspace

Foreign intelligence services increasingly use the Internet and cyber techniques to conduct espionage

Cyber can be an attractive method of intelligence gathering for several reasons:

As we become more reliant on the internet, the threat from cyber espionage will increase

To that end the Government has published a UK Cyber Security Strategy

It can be more cost-effective than traditional means.

Its remote nature means that those involved have an extra layer of deniability.

The volume of data that can be stolen is potentially immense.



HM Government

# National Cyber Strategy 2022

Pioneering a cyber future with  
the whole of the UK

---



## Pillars and objectives



### Pillar 1 Strengthening the UK cyber ecosystem

1. Strengthen the structures, partnerships and networks necessary to support a whole-of-society approach to cyber.
2. Enhance and expand the nation's cyber skills at every level, including through a world class and diverse cyber profession that inspires and equips future talent.
3. Foster the growth of a sustainable, innovative and internationally competitive cyber and information security sector, delivering quality products and services, which meet the needs of government and the wider economy.



### Pillar 2 Building a resilient and prosperous digital UK

1. Improve the understanding of cyber risk to drive more effective action on cyber security and resilience.
2. Prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens.
3. Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks.



### Pillar 3 Taking the lead in the technologies vital to cyber power

1. Improve our ability to anticipate, assess and act on the science and technology developments most vital to our cyber power.
  2. Foster and sustain sovereign and allied advantage in the security of technologies critical to cyberspace.
  3. Secure the next generation of connected technologies and infrastructure, mitigating the cyber security risks of dependence on global markets and ensuring UK users have access to trustworthy and diverse supply.
  4. Work with the multistakeholder community to shape the development of global digital technical standards in the priority areas that matter most for upholding our democratic values, ensuring our cyber security, and advancing UK strategic advantage through science and technology.
- 2a. Preserve a robust and resilient national Crypt-Key enterprise which meets the needs of HMG customers, our partners and allies, and has appropriately mitigated our most significant risks including the threat from our most capable of adversaries





## **Pillar 4**

### **Advancing UK global leadership and influence**

1. Strengthen the cyber security and resilience of international partners and increase collective action to disrupt and deter adversaries.
2. Shape global governance to promote a free, open, peaceful and secure cyberspace.
3. Leverage and export UK cyber capabilities and expertise to boost our strategic advantage and promote our broader foreign policy and prosperity interests.



## **Pillar 5**

### **Detecting, disrupting and deterring adversaries**

1. Detect, investigate and share information on state, criminal and other malicious cyber actors and activities in order to protect the UK, its interests and its citizens.
2. Deter and disrupt state, criminal and other malicious cyber actors and activities against the UK, its interests, and its citizens.
3. Take action in and through cyberspace to support our national security and the prevention and detection of serious crime.



**We will revisit cyber later on, but now let's look at some science and related things.**

**There are two spy museums that have some excellent exhibits**

**You come face to face with spies and spymasters, gadget makers, scientists and engineers from past and present**

# Spy Museum – Washington DC

## FEATURED EXHIBITS

- Spies and Spymasters - reflecting various periods in history, places and spy types. Featured in the profiles are: **Morten Storm, Dmitiri Bystrolyotov, Mata Hari, Sir Francis Walsingham, James Lafayette, Mosab Yousef and Gonen ben Itzhak.**
- Tools of the Trade – The gadgets featured in this exhibit cover **five key areas: covert communications, surveillance and counter-surveillance, escape and evasion, disguise, and secret entry.**
- Looking, Listening, Sensing - featured: Signals Intel (SIGINT), Imagery Intel (IMINT), Measures & Signature Intel (MASINT) and Open Source Intel (OSINT).

# SURVEILLANCE & COUNTERSURVEILLANCE



**SURVEILLANCE & COUNTERSURVEILLANCE:  
LISTENING IN**

PLANNING ELECTRONIC  
INTERCEPTION  
METHODS OF TECHNICAL  
COUNTERSURVEILLANCE



**Meet the lipstick pistol, used by KGB operatives during the Cold War. The 4.5 mm, single shot weapon was small enough to be slipped past even the most suspicious border guards. It fires by pressing the barrel into the victim. The lipstick pistol delivered the ultimate “kiss of death.”**





When an American diplomat in an East European country sent his shoes out for repair, the local counterintelligence service secretly outfitted them with a hidden microphone and transmitter.

During World War I, pigeons were outfitted with tiny cameras and released over enemy territory



Since the earliest days of espionage, pigeons have been a spy's best friend



Distinguished by their speed and ability to return home in any weather, pigeons carried precious, tiny cargo high above enemy lines



During both world wars, radio communication was often unreliable...but troops could count on the pigeon post



Scrotum Alert!!!





This prototype (never used in the field) was specifically designed to be used by downed male pilots to conceal a small escape radio

Male security guards, it was thought, would not thoroughly search the genital area.



In 1945, a group of Soviet children visited the US Embassy in Moscow and gave the Ambassador a hand-carved Great Seal of the USA



It stayed in his office until 1952... when technicians discovered a remarkable listening device inside



With no battery or circuits, how did it transmit? After two months, British Tech Ops finally figured it out



It was a “passive cavity resonator,” activated by a radio beam from a van outside



When people spoke, sound waves entered through tiny holes under the eagle’s beak



These vibrated a membrane that modulated the radio beam, bouncing it back as an audio signal to the people listening in the van



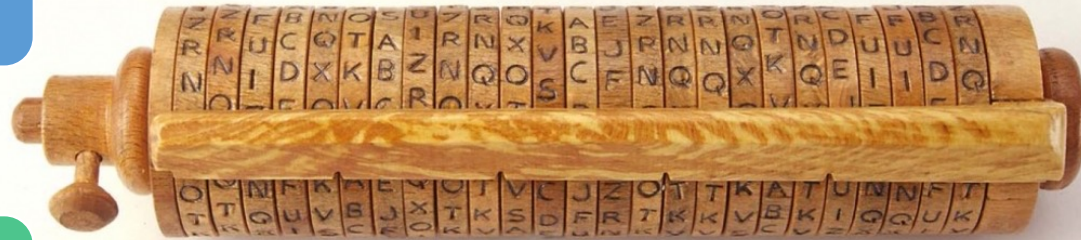
Invented by Thomas Jefferson, this wheel decipher was a way to transfer messages between allies using a special code



The ingenious cylindrical cipher was a secure method to encode and decode messages



Nearly 150 years later, the U.S. Army used a similar device, the M-94, to encrypt messages until early in World War II.





Developed in the 1920s, the Kryha was a clockwork-driven mechanical device for encryption and decryption



In 1933, the U.S. Army was asked to evaluate the security of the device



The challenge message, 1135 characters long, was deciphered in 2 hours and 41 minutes

Bra Alert!!!

A spy in a classic trench coat might easily conceal a camera



But what about a female agent in a dress?



Four female Stasi employees devised a solution: an ingenious bra, code-named "Meadow"



Designed to be worn with a summer dress, its built-in sub-miniature camera controlled by a remote release held in the pocket







**When activated, this device would jam all radio communications around it then self-detonate after its cycle was complete**



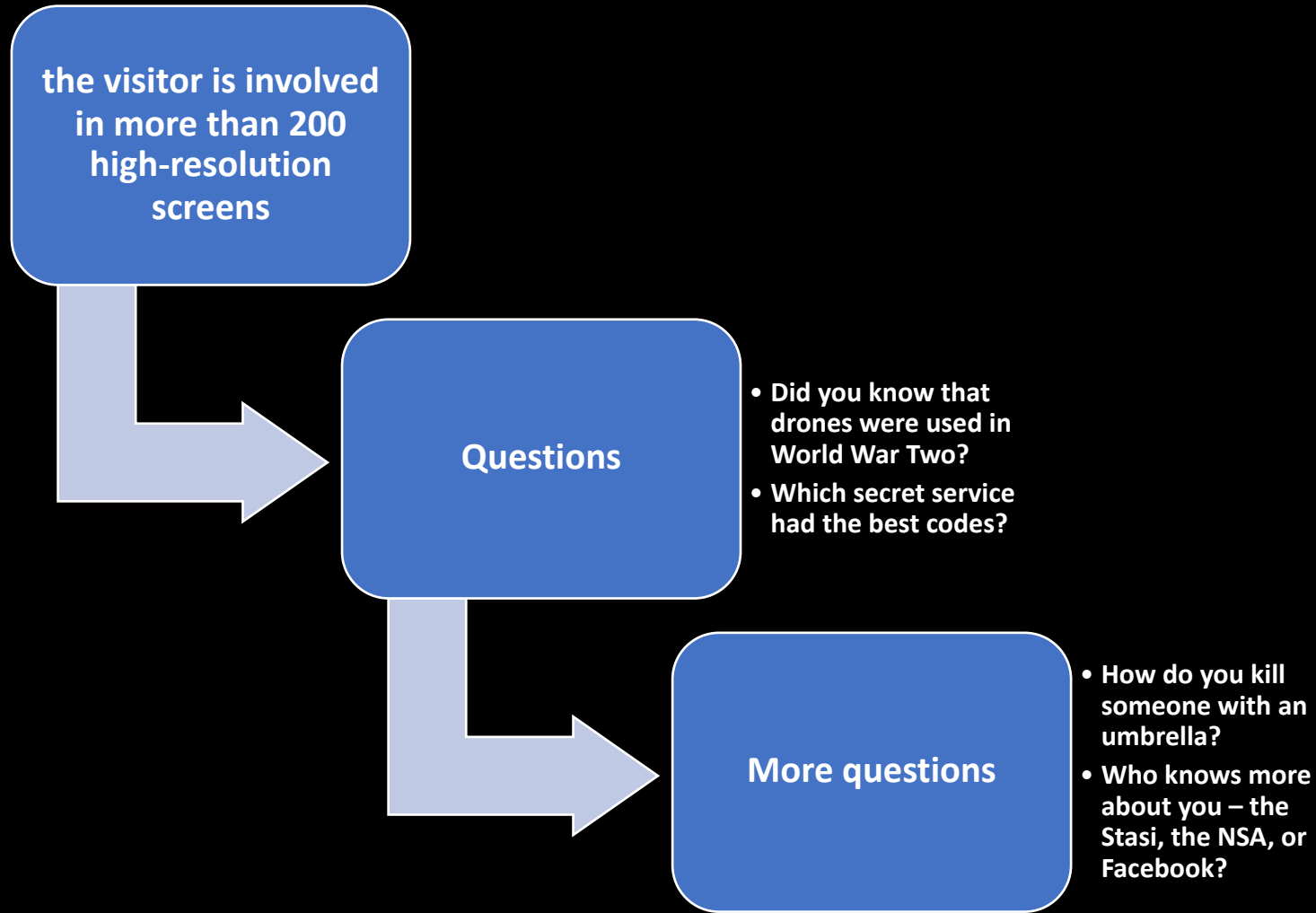
**This solar powered concealment device was used to intercept radar & communications signals**

**US intelligence designed the device to look like a tree stump and then planted it in a wooded area near Moscow**

**A bug inside eavesdropped on radar and communications from a nearby Soviet airbase**

# German Spy Museum - Berlin

The guests of the German Spy Museum Berlin can see, feel, read, hear and smell, what happened in thousands of years of espionage





Intelligence agencies are well-versed in hiding cameras in a range of clandestine locations

The location of hidden cameras should be adapted to the appearance of the agent, so as to allay all possible suspicion

An agent should only use a camera in a box of matches, if they are a smoker

Female KGB agents were issued with a camera installed in a regular lipstick.

The German Spy Museum has an example from the 1980s, the ZVOUK lipstick camera.



# The M-125-3 Fialka cipher machine – the Russian Enigma

In many senses the M-125 represents a further development of the Enigma.



Successor models incorporated further features designed to increase the level of encryption safety



The increase from three discs to ten increased the number of possible combinations from Enigma's 17,576 to a breath-taking 590,490,000,000,000



The Fialka was used by several Warsaw Pact states



Fialka's easy operation and complex encryption meant that it remained in service up to the end of the 1980s



# Finding the truth on the graph

Treachery, a false identity or simple lies are part and parcel of the intelligence world



Seeking to separate the sheep from the goats, a number of countries make considerable use of polygraph tests, more commonly known as "lie detectors"



It is not universally accepted as being reliable.



The Lafayette model 76056 polygraph was used by various US intelligence in the 1970s.



The surveillance of enemy communications has played an important role in military intelligence



The expansion in communications technologies during the 19<sup>th</sup> century created opportunities to spy on the enemy, especially in war time



Mobile field telephones were deployed from the early 20<sup>th</sup> century to link forward units with command headquarters.



One of the first methods of surveillance of these new communications was developed by the Austro-Hungarian Empire



Designed for the Imperial Austro-Hungarian Army, the *Abhorchapparat BW Poppr* functioned as an amplifier of the electrical signals



It was developed as a device which picked up and amplified the electrical signals which seeped into the soil from the telephone cables



# Intelligence Gathering Disciplines

## HUMINT

Human intelligence (HUMINT) are gathered from a person in the location in question. Sources can include the following:

Advisors working with host nation forces

Diplomatic reporting by accredited diplomats

Espionage clandestine reporting

Non-governmental organizations (NGOs)

Prisoners of war (POWs) or detainees

Refugees

Routine patrolling

Special reconnaissance

## **GEOINT**

**Geospatial intelligence (GEOINT) are gathered from satellite and aerial photography, or mapping/terrain data.**

## **IMINT**

**Imagery intelligence – gathered from satellite and aerial photography**

## **MASINT**

**Measurement and signature intelligence (MASINT) are gathered from an array of signatures (distinctive characteristics) of fixed or dynamic target sources. MASINT is split into six major disciplines: electro-optical, nuclear, radar, geophysical, materials, and radiofrequency.**

**Electro-optical MASINT**

**Airborne electro-optical missile tracking MASINT**

**Infrared MASINT**

**Optical measurement of nuclear explosions**

## **OSINT**

**Open-source intelligence (OSINT) are gathered from open sources. OSINT can be further segmented by the source type: Internet/General, Scientific/Technical, and various HUMINT specialties, e.g. trade shows, association meetings, and interviews.**

## **SIGINT**

**Signals intelligence (SIGINT) are gathered from interception of signals.**



## **Communications intelligence (COMINT)**

Electronic intelligence (**ELINT**) – gathered from electronic signals that do not contain speech or text (which are considered COMINT)

Foreign instrumentation signals intelligence (**FISINT**) – entails the collection and analysis of telemetry data from a missile or sometimes from aircraft tests; formerly known as telemetry intelligence or TELINT

## **TECHINT**

Technical intelligence (**TECHINT**) are gathered from analysis of weapons and equipment used by the armed forces of foreign nations, or environmental conditions.

Medical intelligence (**MEDINT**) – gathered from analysis of medical records and/or actual physiological examinations to determine health and/or particular ailments and allergic conditions for consideration

## **CYBINT/DNINT**


Cyber or digital network intelligence (CYBINT or DNINT) are gathered from cyberspace. CYBINT can be considered as a subset of OSINT.

## **FININT**


Financial intelligence (FININT) are gathered from analysis of monetary transactions.

# Back to Cyber


A wide array of bad actors is leveraging technology to threaten across vast distances




China is launching massive cyberattacks to steal intellectual property



and building space weapons to cut off military satellite communications before the fighting ever starts.



Russia is using Facebook, Twitter, and other social media platforms to wage information warfare



Three dozen countries have autonomous combat drones and at least nine have already used them.

The most serious threats from a national security perspective come from well-trained operatives and proxies operating at the behest of four countries

China

Russia

Iran

North Korea.

Together, these four nations are behind 77 percent of all suspected state-sponsored cyberattacks since 2005.

While running a wide range, the cyberattacks perpetrated by China, Russia, Iran, and North Korea come in five basic types:

stealing

spying

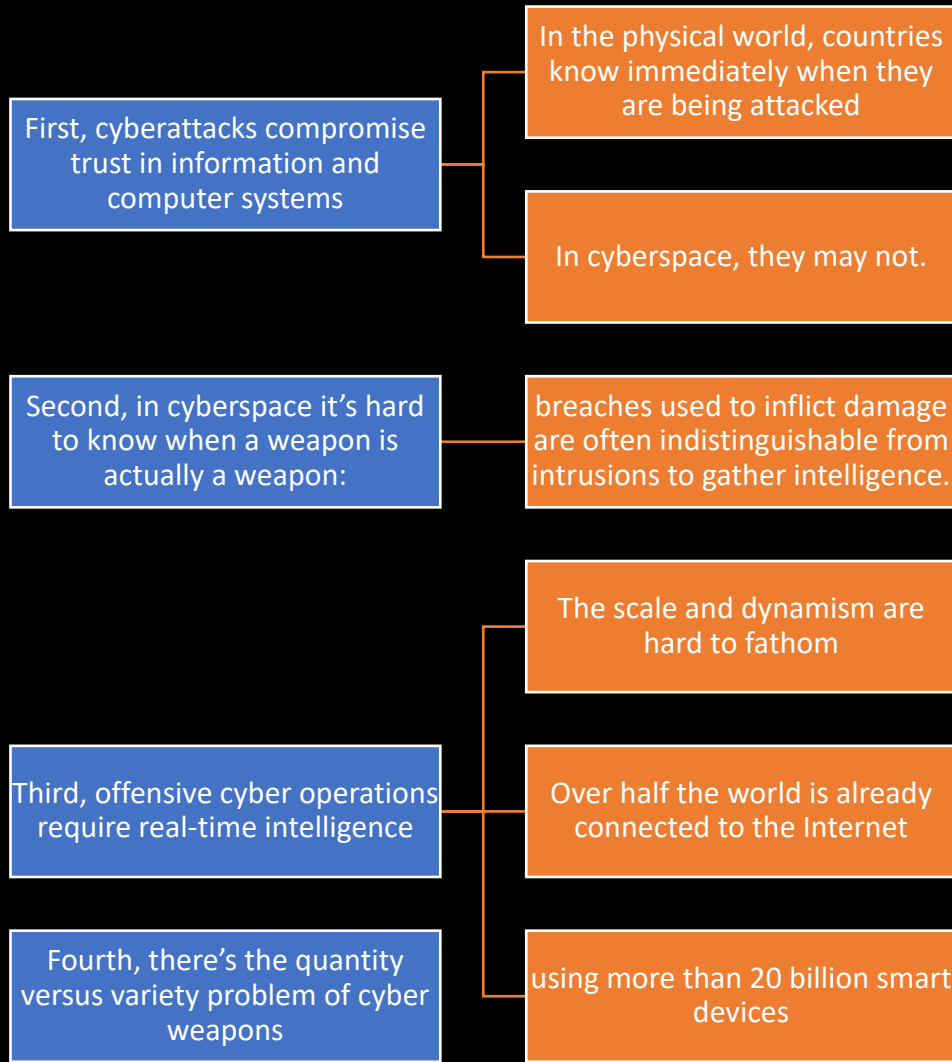
disrupting

destroying

deceiving.

# What Does Intelligence Have to Do with Cyber?

Four features of the evolving cyber landscape are placing unprecedented demands on intelligence



# How Technology is Changing the Future of Espionage

## Biometrics

One element of tradecraft is utilizing a cover.

The clandestine operative assumes a false identity with a fake passport, which helps him infiltrate a foreign country.

However, with the advent of biometric technology such as fingerprint scanners, widely used in airports and customs control points around the world, spies may need to adjust their tradecraft or develop entirely new techniques.

Because of the proliferation of biometric technology, our highly trained spies may become single-use operatives.

Once their biometrics are collected abroad, they can never be used for clandestine work again.

# How Technology is Changing the Future of Espionage

## Social media

How hard will it be for intelligence services to recruit spies who have zero social media presence?

Intelligence Agencies will have a tough time finding a 30-year-old recruit who has never travelled abroad (where their biometrics may have been gathered) and who has never posted his or her pictures on social media.

# How Technology is Changing the Future of Espionage

## Metadata

```
graph TD; A[Metadata] --> B[Rather than simply look at the actual contents of phone conversations, text messages, and emails, metadata is the underlying technical information used to make those transactions possible]; B --> C[contains information about how, when, and where you communicate from]; C --> D[This type of information can be analyzed and used by intelligence professionals in many different ways.]; D --> E[Another aspect of tradecraft is running surveillance detection routes (SDRs) to spot counterintelligence agents and allow our spies to meet with their assets in a clandestine manner]; E --> F[Obviously, this becomes highly problematic when foreign governments are tracking metadata emitted by our mobile phones.];
```

Rather than simply look at the actual contents of phone conversations, text messages, and emails, metadata is the underlying technical information used to make those transactions possible

contains information about how, when, and where you communicate from

This type of information can be analyzed and used by intelligence professionals in many different ways.

Another aspect of tradecraft is running surveillance detection routes (SDRs) to spot counterintelligence agents and allow our spies to meet with their assets in a clandestine manner

Obviously, this becomes highly problematic when foreign governments are tracking metadata emitted by our mobile phones.



# How Technology is Changing the Future of Espionage


The birth of a new form of espionage?



Technology can always be defeated with greater technology



Biometric sensors can be spoofed if intelligence agencies are able to gain access to the programming that its software operates on and start changing around the ones and zeroes in the code.



In the future, robots may do most of the spying for us.



It could be our kitchen appliances spying on us tomorrow, and that isn't an exaggeration.



The proliferation of technology may give rise to a new form of intelligence gathering, a new type of 'int.'



The spy of the future may be a high-speed cable repairman whose function is to emplace technology near the person or people we need to collect information from.

# How Technology is Changing the Future of Espionage

## Bioengineered spies

```
graph TD; A[Bioengineered spies] --> B[Perhaps sometime in the not-so-distant future, nations will engineer operatives from birth for the purpose of espionage.]; B --> C[While it may sound outlandish at the moment, we are already on the cusp of several new technologies likely to alter the way we live even more dramatically than the invention of the Internet and telecommunications technologies]; C --> D[In the coming decades, biometric scanners, statistical analysis of big data, are likely to make it much more difficult to place spies under a cover and have them conduct covert activities]; D --> E[A spy can change a lot of things about him or herself for purposes of deception, but not their DNA, and DNA scanners may be one of the key technologies mentioned above.];
```

Perhaps sometime in the not-so-distant future, nations will engineer operatives from birth for the purpose of espionage.

While it may sound outlandish at the moment, we are already on the cusp of several new technologies likely to alter the way we live even more dramatically than the invention of the Internet and telecommunications technologies

In the coming decades, biometric scanners, statistical analysis of big data, are likely to make it much more difficult to place spies under a cover and have them conduct covert activities

A spy can change a lot of things about him or herself for purposes of deception, but not their DNA, and DNA scanners may be one of the key technologies mentioned above.