Hillingdon U3A Computer Group

GOVERNMENT COMMUNICATIONS HEADQUARTERS

SECRET SERVICE BUREAU

Home Section

Foreign Section

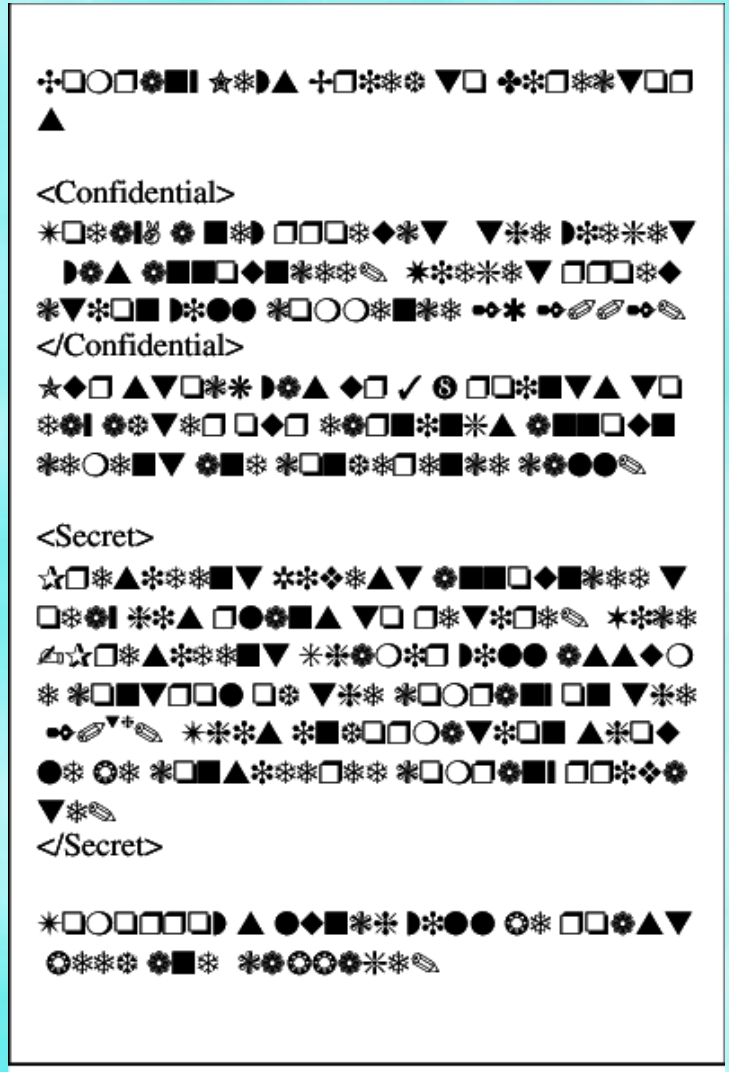
THE GREAT WAR (1914 – 1918)

Signal Intelligence

To be good at SIGINT you need to be able to:

1. Intercept Messages

2. Break the cipher code and decrypt the coded message.



Naval and Military Signals Intelligence

Zimmermann Telegram to Germany's ambassador in Mexico

Jan 1917.

WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310

18147 18222 21560 10247 11518 23677 13605 3494 14936

98092 5905 11311 10392 10371 0302 21290 5161 39695

23571 17504 11269 18276 18101 0317 0228 17694 4473

23284 22200 19452 21589 67893 5569 13918 8958 12137

1333 4725 4458 5905 17166 13851 4458 17149 14471 6706

13850 12224 6929 14991 7382 15857 67893 14218 36477

Government Code & Cypher School (GC&CS) formed in 1919 based in London at Watergate House.

During World War II, GC&CS moved from London to Bletchley Park.

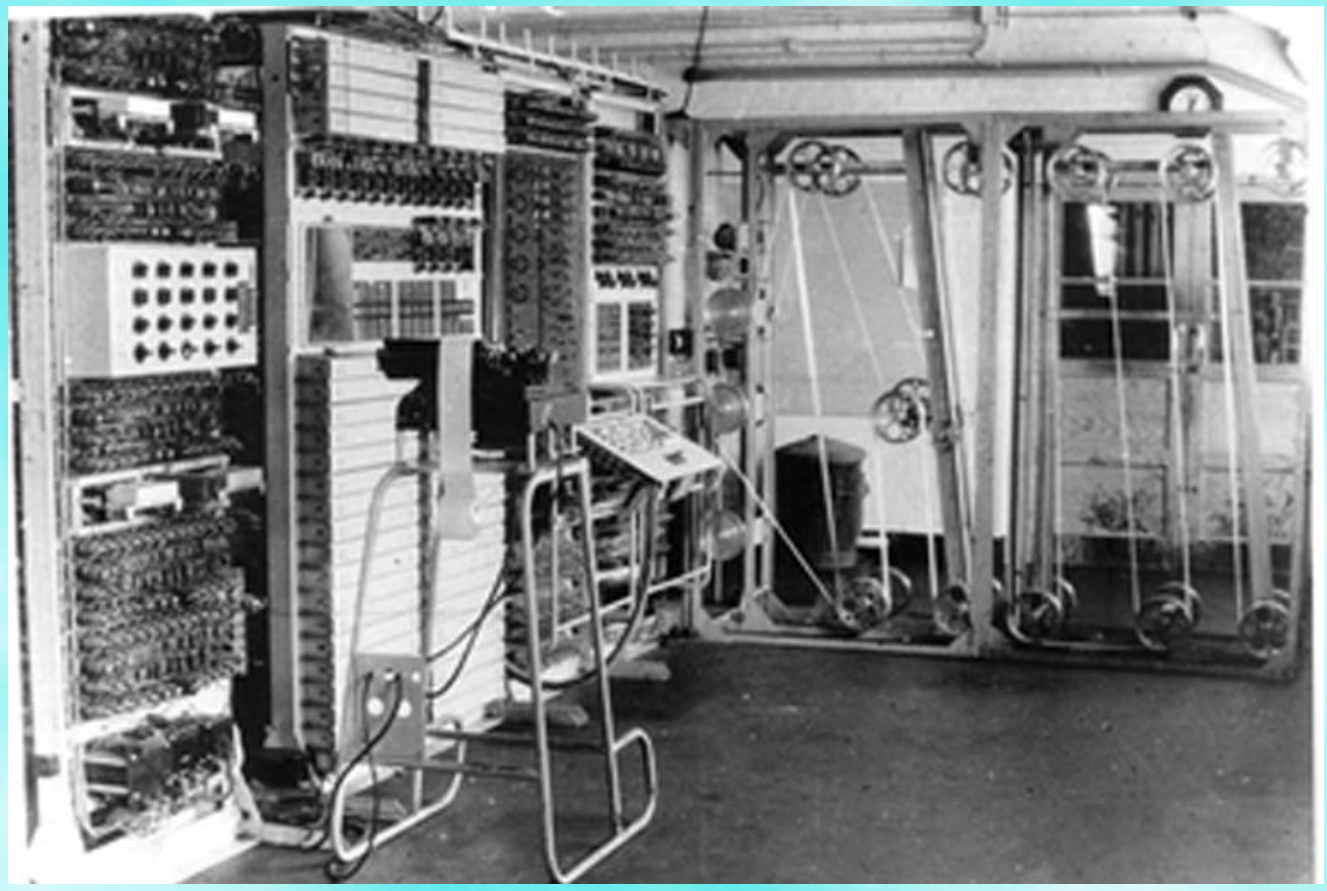
Soon after the move GC&CS became the **Government Communications Headquarters** (GCHQ).

Intercepted encrypted enemy messages were sent to Bletchley Park where teams of codebreakers attempted to break the cipher codes to be able to read the messages.

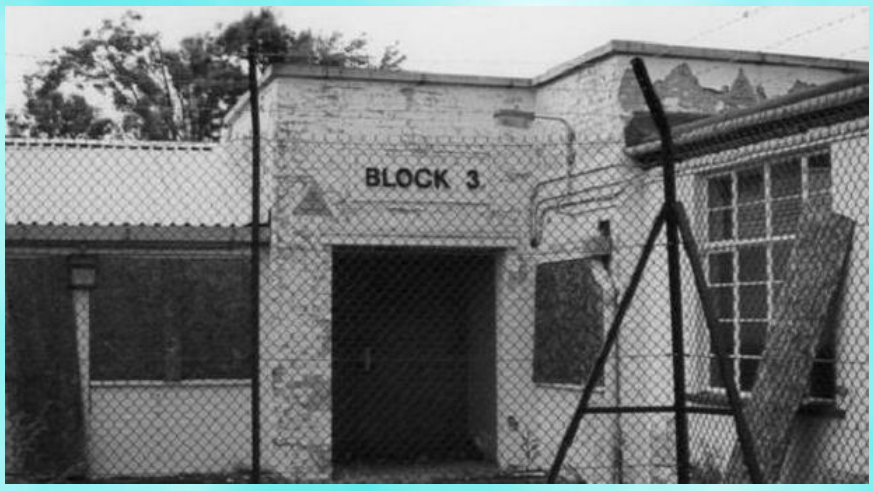
Lorenz

Enigma

The first electronic computer, the COLOSSUS, was designed and built to help in the cryptanalysis of intercepted enemy messages sent using the Lorenz cipher.



In 1946, GCHQ moved to **RAF Eastcote**, also known as **RAF Lime Grove**



Then in 1952 it moved to the suburbs of **Cheltenham**.

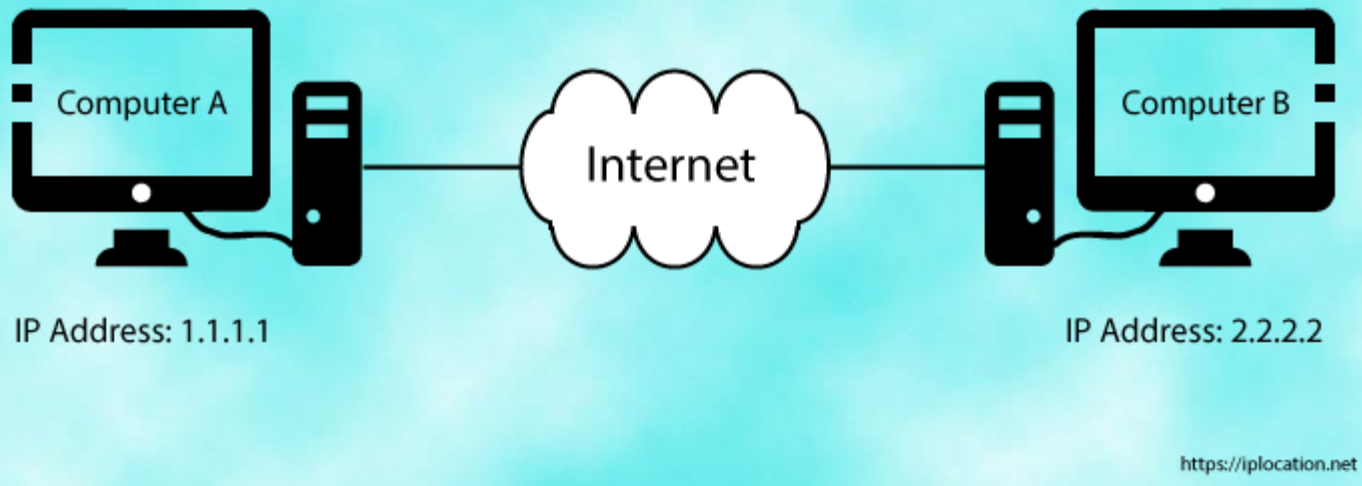
INTERNET INTELLIGENCE DATA COLLECTION

With the birth of the World Wide Web, intercepting internet communications is much more complex than intercepting telegrams, postal or radio communications.

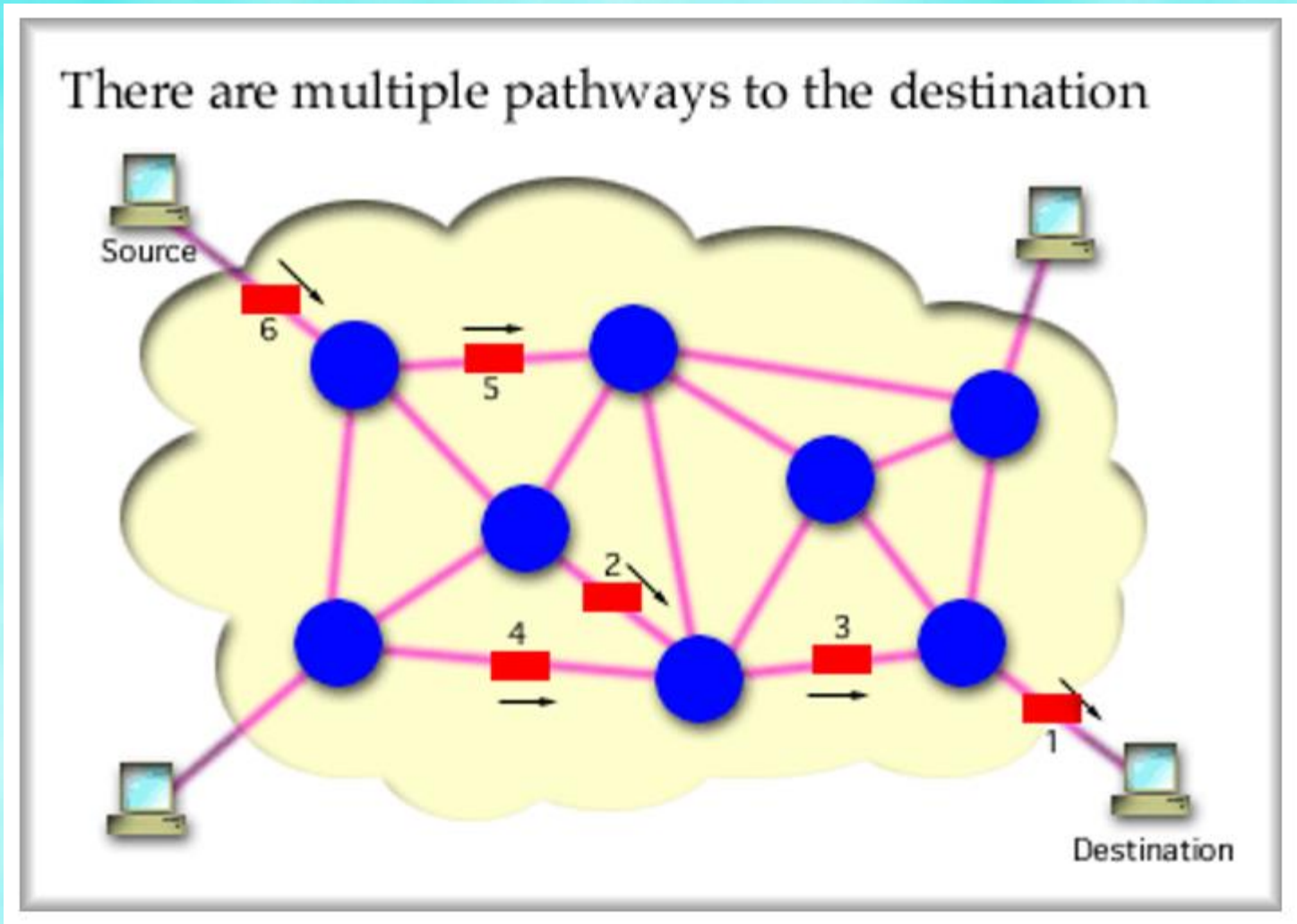
MESSAGE SENDER AND RECIPIENT

In daily life, to enable people to communicate with each other, we need a unique postal address and a unique telephone number.

To ensure a computer receives its intended internet communications, it also needs an unique address, called an **Internet Protocol Address** (IP Address)



INTERNET DATA PACKETS

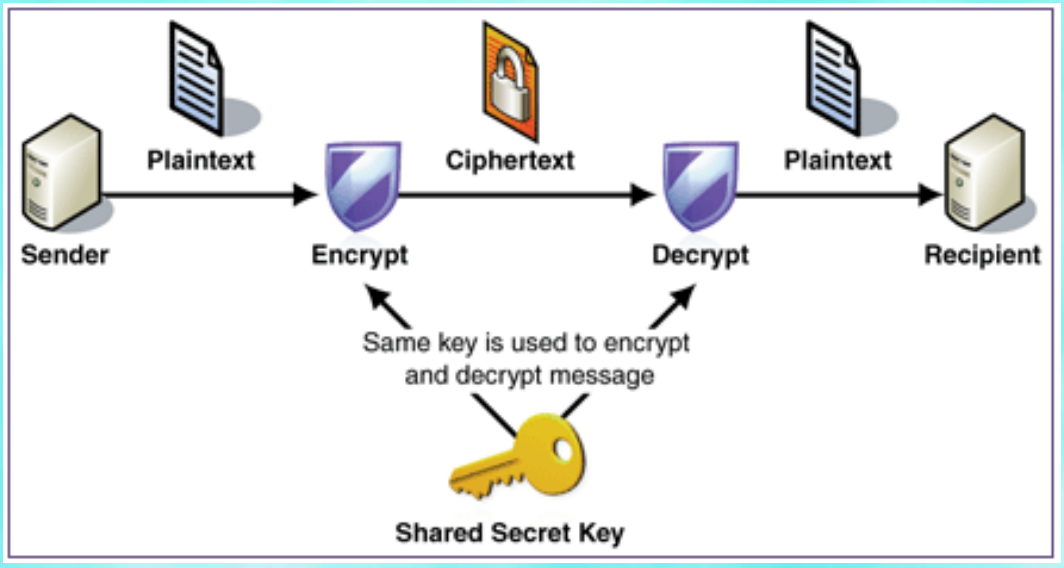


INTERNET DATA ENCRYPTION

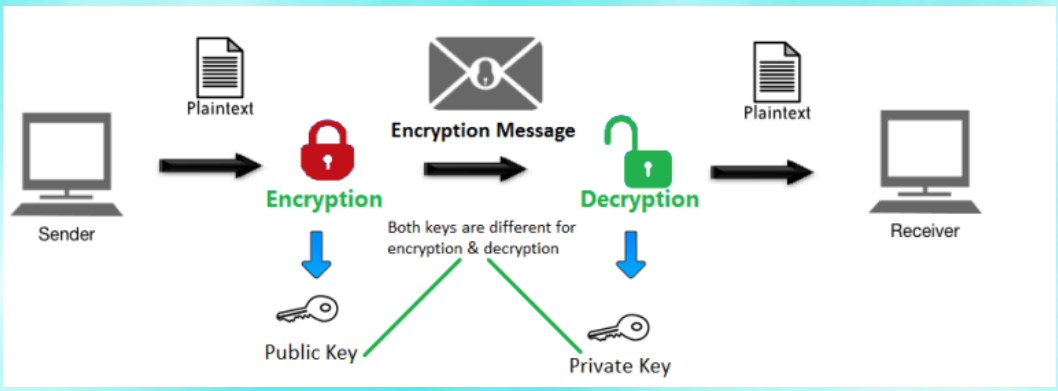
For data protection, most websites encrypt data when it is being sent to and from a website.

Look for the padlock icon in the URL bar, and the “s” in the “https://”.

Two of the most widely used encryption algorithms today are AES and RSA. Both are highly effective and secure.



AES



RSA

Since the introduction of the internet, GCHQ has had to shift from Cold war-era SIGINT listening posts, to digital surveillance for collecting Communications Intelligence (COMINT) data.

EDWARD SNOWDEN

Reference: OPC-M/TECH.A/455 (v1.0, r206)
Date: 20 September 2011
Copy no:

HIMR Data Mining Research Problem Book

[redacted]
OPC-MCR, GCHQ

Summary
In this problem book we set out areas for long-term data mining research at the Heilbronn Institute for Mathematical Research starting in October 2011 and continuing for at least three years. The four areas are beyond supervised learning, information flow in graphs, streaming exploratory data analysis and streaming expiring graphs.

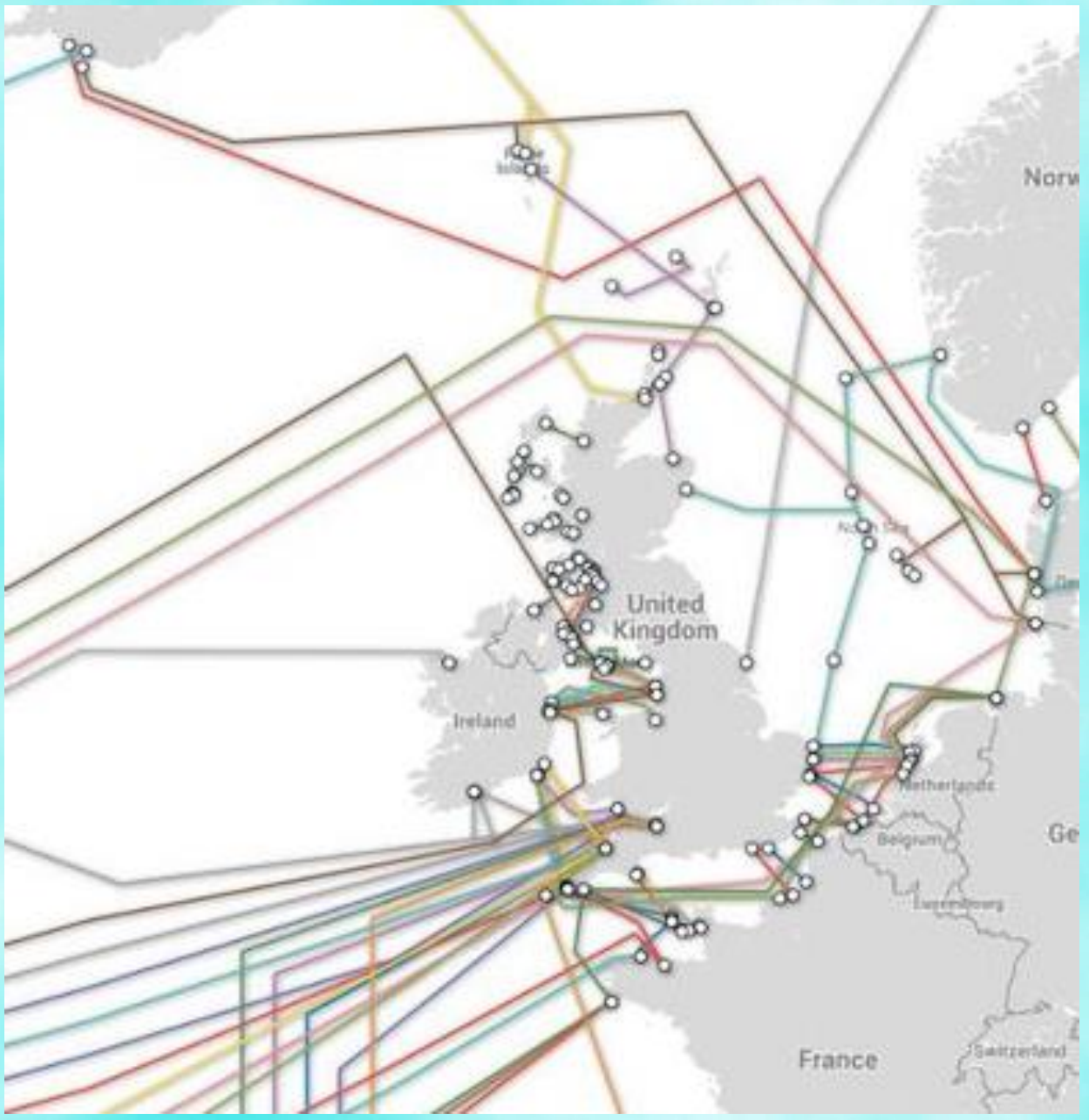
Copy	Distribution
1	NSA R1 [redacted]
2	NSA R4 [redacted]
3	NSA R6 [redacted]
4	LLNL [redacted]
[redacted]	[redacted]
6	CSEC [redacted]
7	CRI [redacted]
8	DSD [redacted]
9	GCSB [redacted]
10	ICTR [redacted]
11	ICTR-CISA [redacted]
12	ICTR-DMR [redacted]
13	ICTR-MCA [redacted]
14	NDIST [redacted]
15	IAC7T [redacted]
16	PTD [redacted]
17	HIMR (circ.)
18	OPC-MCR (circ.)

THE BLACK HOLE

This is a massive GCHQ database repository.

TEMPORA

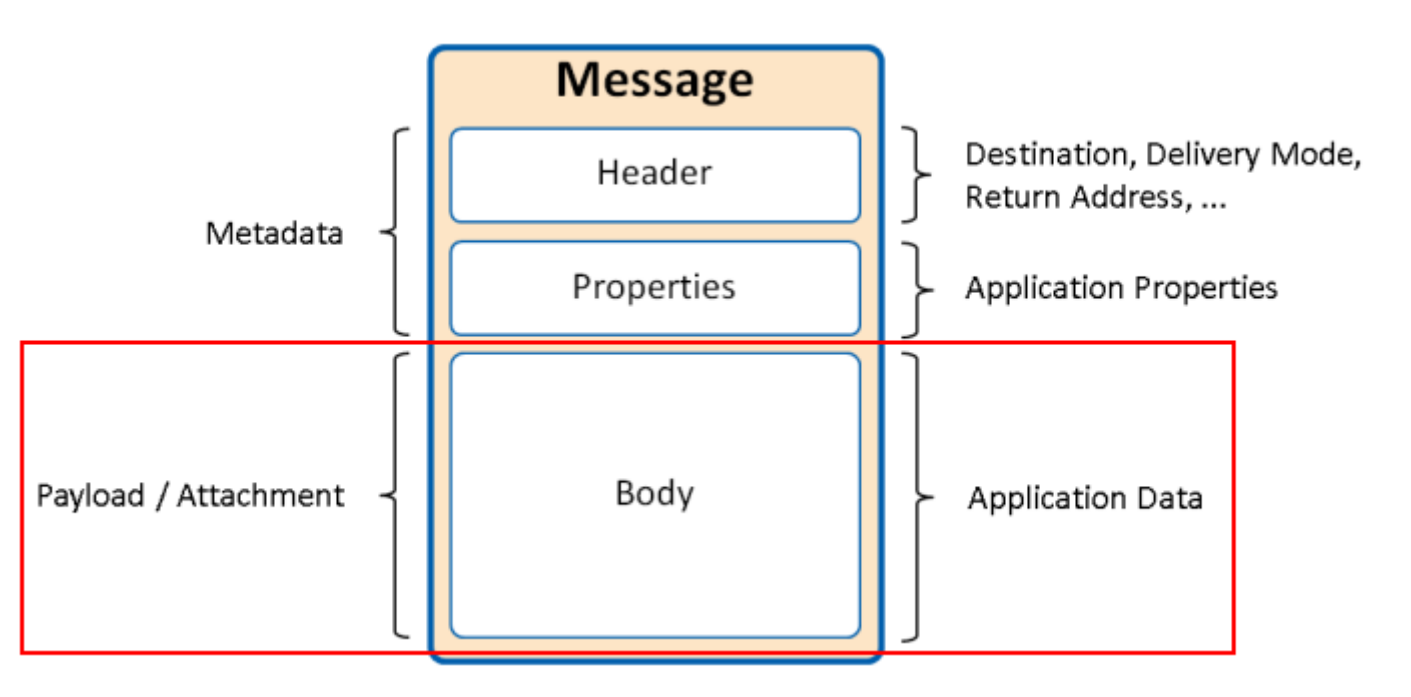
GCHQ intercepts fibre-optic communications cables in and out of the UK.



KARMA POLICE

Monitors the internet and collects the IP addresses of any individual visiting websites, as well as the associated cookies and stores them in the BLACK HOLE.

METADATA ANALYSIS



MEMORY HOLE

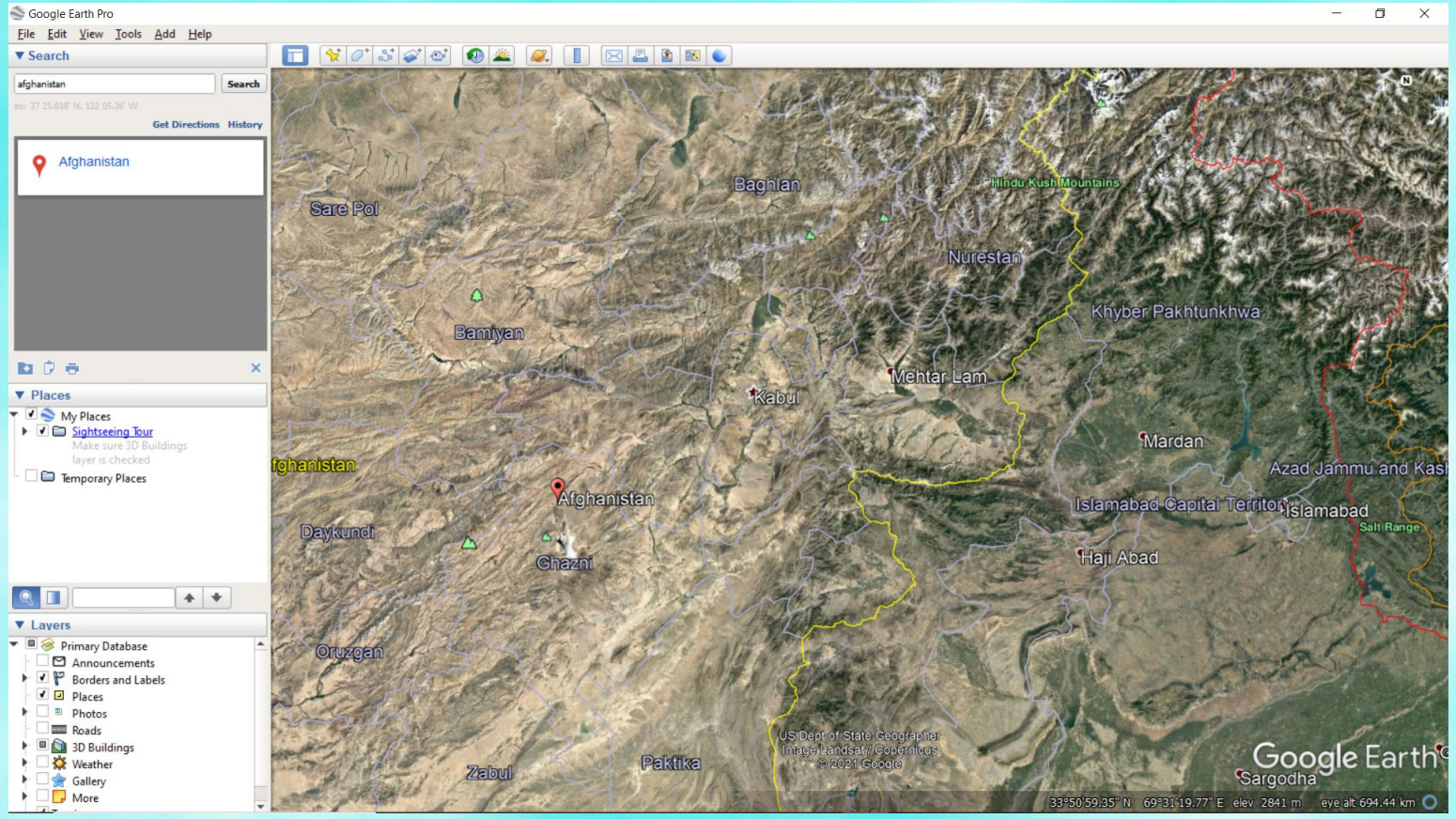
Analyses BLACK HOLE information on web searches made on engines such as Google's. It provides information on when, where, and from which IP addresses particular searches were made.

MUTANT BROTH

Used to analyse vast amounts of tiny Internet data files known as cookies stored in the BLACK HOLE.

MARBLED GECKO

Searches the BLACK HOLE for people's usage of Google Earth and Google Maps.



RADIO RADICALISATION

Collected intelligence about people using the internet to listen to radio shows.

SAMUEL PEPYS

Monitors the content and metadata of online communications and Web browsing activity as they are intercepted in real time for an IP address.

It is used to find out what a target is doing online right now.

OTHER OPERATIONS:

OPERATION SOCIALIST

GCHQ targeted Belgacom, Belgium's largest telecommunications provider, with spyware called Regin. The purpose of the GCHQ hack was to spy on phones and internet users using the Belgacom network.

OPTIC NERVE

In one six month period in 2008, GCHQ spied on 1.8 Million Yahoo webcam chats.

INFINITE MONKEYS

A system used to sift through details about users of online forums.

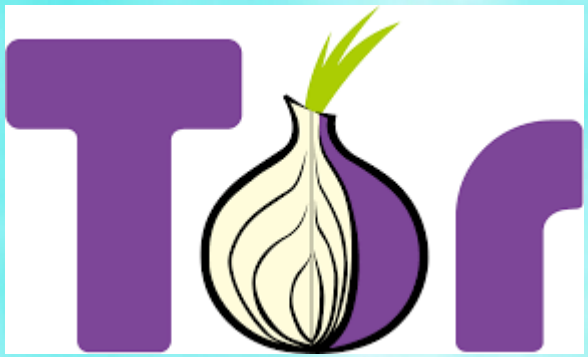
ONLINE VIRTUAL WORLDS

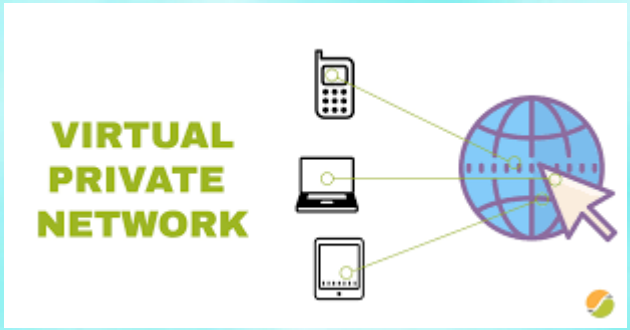
Online games like World of Warcraft and Second Life are environments in which real people meet to play the games.

ENCRYPTED MESSAGE DATA

EDGEHILL

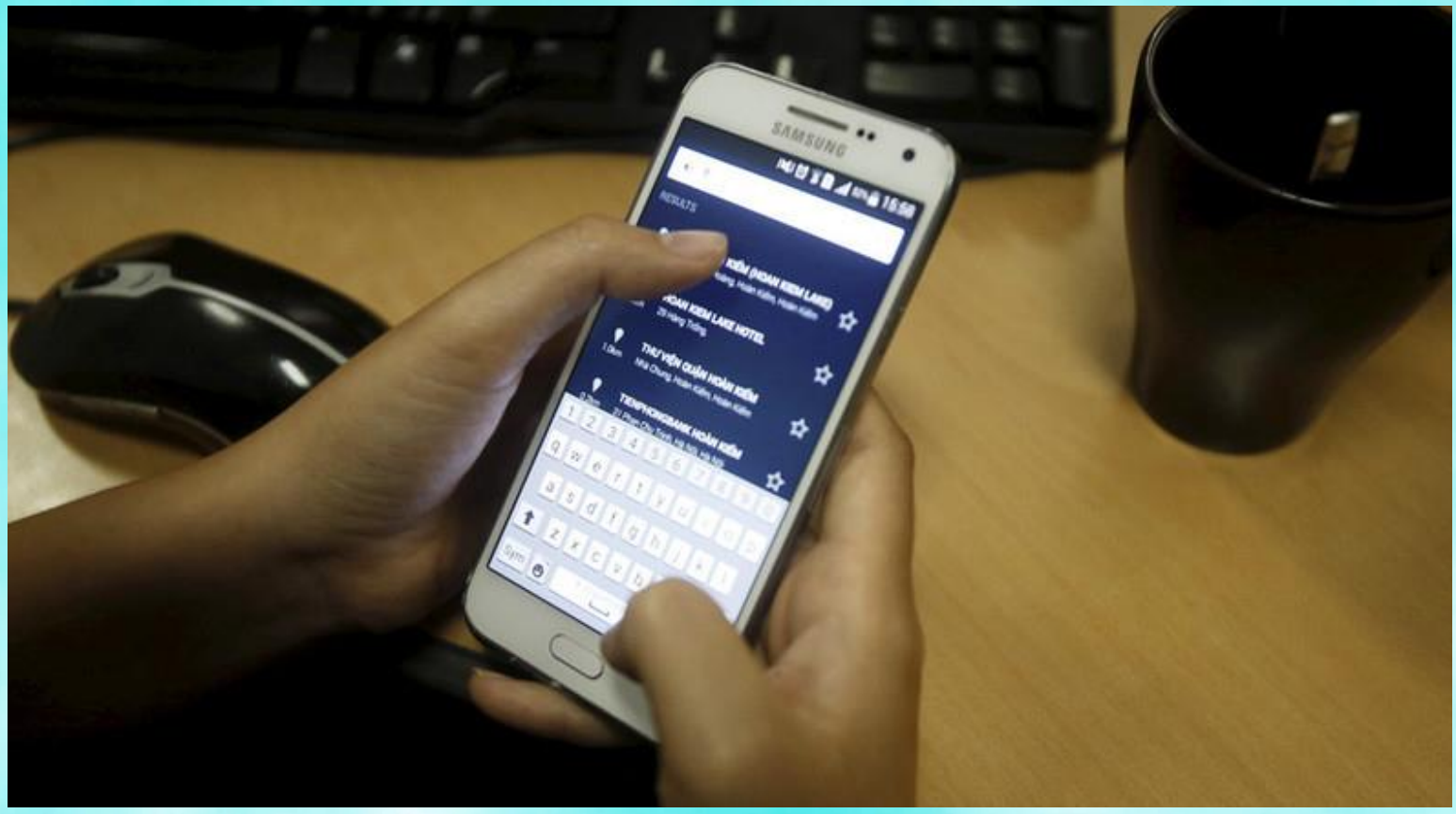
This project was to use Super-computers to crack the algorithms behind the internet encryption codes.





Most of the Snowden revelations are about spying via the internet, but NSA and GCHQ are also conducting the more traditional collection of telephone communications that go through satellite links as well.

SPYING ON SMARTPHONES



THE THREE SMURFS

GCHQ targeted plugin tools against individual smartphones, such as iPhones, Android devices, and other platforms.

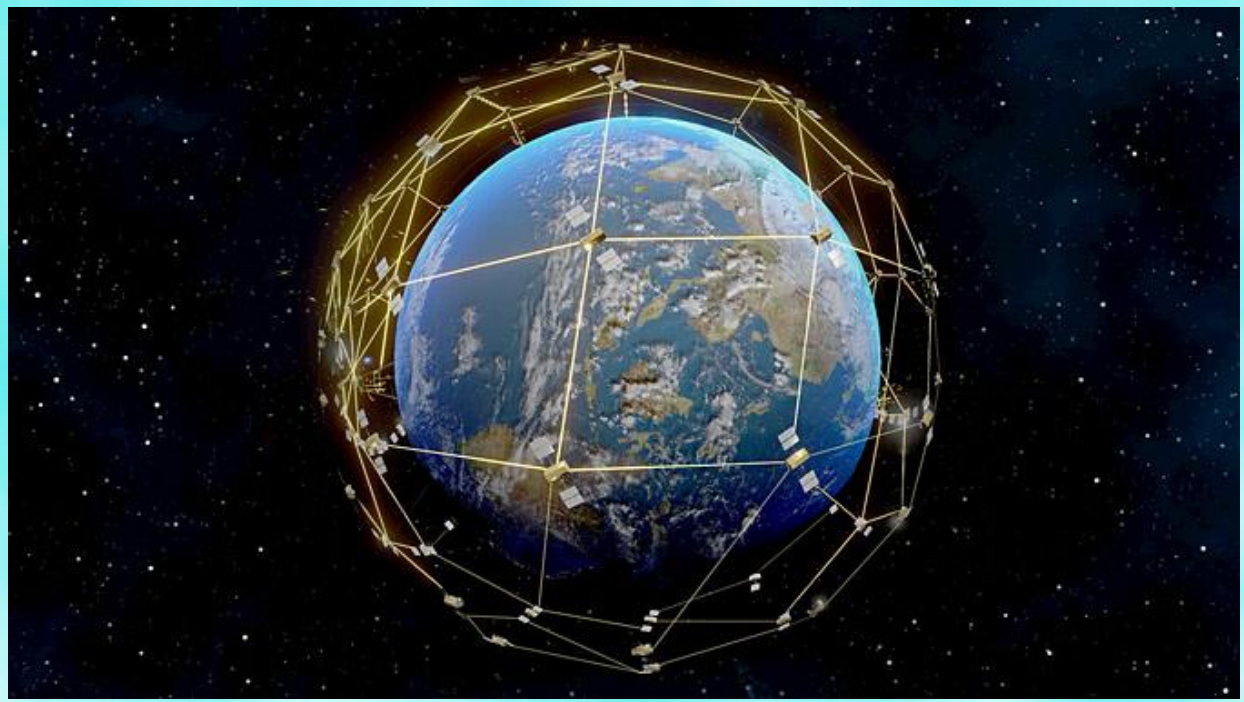
DREAMY

NOSEY

TRACKER

CYBER WARFARE

GCHQ uses its COMINT capability to monitor and spy on worldwide communications.



In the meantime, China, Russia, North Korea and the U.S. are spying very effectively on everyone else.

Cyber Attacks

BBC NEWS | Europe | Estonia hit by 'Mc

http://news.bbc.co.uk/2/hi/europe/6665145.stm

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

E-mail this to a friend Printable version

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Estonia says many state websites have been affected

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.

Russian hackers' cyber disruption of the Ukrainian power supply in 2015.

Russia infected Ukrainian tax software to disable the systems of anyone using it.

Russian interference in the French and US democratic processes by hacking into political parties to steal and leak sensitive material.

Iranian attack aimed at affecting the functioning of Israeli water treatment plants.

Iranian attacks that disabled 30,000 computers belonging to Saudi Aramco in 2012

North Korea blamed for unleashing the WannaCry cyber attack that crippled hospitals, banks and other companies across the globe in 2017.

JOINT THREAT RESEARCH INTELLIGENCE GROUP

They have a large range of tools of which the following are just a small sample:

CHANGELING - Ability to spoof any email address and send email under that identity.

TORNADO ALLEY - a delivery method (Excel Spreadsheet) that can silently extract and run an executable on a target's machine.

SWAMP DONKEY - a tool that will silently locate all predefined types of file and encrypt them on a targets machine.

ANGRY PIRATE - a tool that will permanently disable a target's account on their computer.

TRACER FIRE - An Office Document that grabs the targets Machine info, files, logs, etc and posts it back to GCHQ.

SUNBLOCK - Ability to deny functionality to send/receive email or view material online.

SPRING BISHOP - Find private photographs of targets on Facebook

NATIONAL CYBER FORCE

Set up in 2020, and drawing its personnel from the Ministry of Defence and the security services including GCHQ and MI6.

Computer have changed our world – and they have changed spying – and will continue to do so in ways we can not predict!