

La Informática y la Guerra

1. Alan Turing.
2. Máquina de Turing:
 - Características.
 - Configuración.
3. Código Enigma.
4. Máquina Colossus:
 - Características.
 - Programación primitiva.
5. Contrainformática.
6. Ataque de Comando y Control: Explotación de la informática como arma ofensiva.
 - ☒ Tipos de Guerra:
 - ☑ Guerra Electrónica.
 - ☑ Ciberguerra.
 - ☑ Guerra de la Información (GI):
 1. Concepto.
 2. Actividades Ofensivas de la GI:
 - Espionaje.
 - Sabotaje.
 - Echelon.

Alan Turing.

"El inglés Alan Turing (1912-1954) puede ser considerado el padre de la Inteligencia Artificial (IA), aunque este nombre no se usase hasta después de 1956. Turing estudió lógica matemática en la Universidad de Cambridge y en 1937 estuvo en el Institute for Advanced Studies de Princeton, donde estaban Gödel y Von Newman, entre otros destacados lógicos y matemáticos, además de Albert Einstein. Durante la segunda guerra mundial trabajó para su país en los servicios de información; en 1949 en la Universidad de Manchester y en el programa MADAM (Manchester Automatic Digital Machine) que resultó ser el equipo de computación de mayor memoria construido hasta entonces. Condenado a causa de su homosexualidad a un tratamiento, o tortura, médico-farmacéutica equivalente a la castración, Turing se suicidó por envenenamiento en 1954." (Enric Trillas50-51).

"Durante los años de la segunda guerra mundial, Turing colaboró en el diseño de una máquina llamada la 'Bomba' que exploraba las combinaciones posibles generadas por la máquina codificadora alemana 'Enigma'. Tal 'Bomba' fue una máquina de propósito especial, el de descifrar códigos, construida electromecánicamente con relés. Asimismo, trabajó en el desarrollo de la 'Colossus' (que algunos consideran como el primer ordenador electrónico) que ya funcionaba con válvulas (tubos de vacío) en lugar de relés; gracias a ella los británicos pudieron mantener alejados de los submarinos alemanes a los barcos de suministro que cruzaban el Atlántico... Turing no recibió en vida reconocimiento alguno de la sociedad a la que tanto ayudó en los momentos más difíciles." (Enric Trillas51)

"Más sorprendente todavía es que Turing demostró que para cualquier sistema de sus máquinas que sea necesario para efectuar algoritmos cada vez más complicados existe una máquina de Turing capaz de hacerlo todo ella sola. Tal máquina hipotética recibe el nombre de 'máquina de Turing universal', y su existencia teórica pone de manifiesto que el concepto de máquina de Turing es de una versatilidad sin fin, al permitir que cualquier incremento de la complejidad del algoritmo pueda ser aceptado por una lista más larga de especificaciones... Los ordenadores actuales son realizaciones de las ideas de John von Neumann y de Alan Turing." (Enric Trillas53)

Turing "en 1950 propuso una prueba que se conoce como el 'test de Turing', el cual se basa en la idea siguiente: si una persona se comunica sólo a través de un terminal con otras dos partes, que están escondidas, y no se puede discriminar a través de preguntas cuál de ambas partes es una persona y cuál es un ordenador, entonces no se puede negar que la máquina muestra la cualidad que, en las personas, se llama 'inteligencia'. Tal procedimiento tiene la ventaja de no tener que definir lo que es la inteligencia. Turing creía firmemente que máquinas que piensen llegarían a existir y predijo que hacia el año 2000 una máquina jugaría al 'juego de imitación', como él llamó al test, de manera que un interrogador medio no tendría más del 70 por 100 de posibilidades de efectuar la identificación correcta tras cinco minutos de preguntas." (Enric Trillas55)

En el desarrollo de la computadora, la teoría antecedió a la práctica. El manifiesto del nuevo orden electrónico de cosas fue un trabajo ("On Computable Numbers" -Sobre números calculables-) publicado en 1936, por el matemático y lógico A.M.Turing, el cual determinó la naturaleza y las limitaciones teóricas de las máquinas lógicas antes de que se construyera siquiera una sencilla computadora por completo programable.(Bolter17).

Turing... en 1950 publicó "Computing Machinery and Intelligence"... expresó su convicción de que las computadoras eran capaces de imitar perfectamente la inteligencia humana y que tal hazaña la realizarían hacia el año 2000.

Al prometer (o al amenazar) sustituir al hombre, la computadora nos ofrece una nueva definición de hombre, como "procesador de información", y de naturaleza, como "información que debe ser procesada".(Bolter18).

"En 1936 Turing concibió su propio autómeta imaginario. La máquina de Turing, como se le llegó a conocer, no hizo intento alguno para unirse a la sociedad de las criaturas vivas. Podría visualizarse más como un tocacintas muy sofisticado con una cinta arbitrariamente infinita. "Siendo una Máquina de Estados Finitos, se podría concebir como un autómeta finito".(Lévy 22-23)

LA MAQUINA DE TURING

Es el primer modelo de cálculo que aparece históricamente.

Siguiendo unas reglas de operación dadas y a partir de unos datos iniciales, realiza operaciones y obtiene unos resultados en un tiempo finito.

CARACTERÍSTICAS:

- Disponer de una cinta infinita por ambos extremos dividida en celdas. Cada celda almacena un símbolo de un alfabeto prefijado.
- Disponer de una cabeza de lectura /escritura móvil que en cada momento accede a una única celda.
- Encontrarse siempre en un determinado estado "q i " de entre un conjunto finito de estados.
- Realizar las siguientes acciones elementales en función del estado en que se encuentre y del símbolo que lea de la cinta:

Reescritura del contenido de la celda leída.

Movimiento de la cabeza a la dcha o izda de la celda leída.

Formalmente una MT está formada por la cuádrupla (Σ , Q, q₀, δ) donde:

- Σ es un conjunto de símbolos que contiene al espacio en blanco (#)
- Q es un conjunto finito de estados.
- q₀ \in Q , es el estado inicial.
- δ es la función de transición:

CONFIGURACIÓN:

Representación del estado y del contenido de la cinta (sólo la parte no vacía). Respecto al contenido de la cinta se indica a qué cuadrado señala la cabeza mediante subrayado.

Ejemplos:

(q₁, 111#11)
(q₀, 1#11##1)

📁 **CONFIGURACIÓN INICIAL:**

Es una configuración cuyo estado es q_0 y la cabeza se encuentra en el primer espacio a la derecha de la cinta, tal que a su derecha todo son espacios

Ejemplo: $(q_0, 111\#111\underline{\#})$

📁 **CONFIGURACIÓN FINAL:**

La que se alcanza cuando se llega a FIN o ERROR. En estos casos la configuración se representa con esa palabra y el contenido de la cinta. En caso de llegar a FIN, la cabeza se deberá encontrar en el primer espacio a la derecha de la cinta tal que a su derecha todo son espacios en blanco.

Ejemplo: $(\text{FIN}, 111\underline{\#})$

$(\text{ERROR}, 11111\underline{1})$

📁 **CÁLCULO EN UN PASO:**

Se pasa de una configuración a otra mediante una transición (flecha doble \implies).

📁 **CÁLCULO EN VARIOS PASOS:**

Consiste en ir de una configuración a otra mediante la aplicación de sucesivas transiciones, lo que implica pasar por sucesivas configuraciones (flecha doble con asterisco \implies^*).

📁 **CÁLCULO COMPLETO:**

Empieza en una configuración inicial y acaba en una configuración final.

Ejercicio de MT para la exposición:

Diseñar una MT que calcule la función suma de dos números naturales representados en unario ($5 = 11111$, $2 = 11$).

- Configuración inicial $(q_0, 11\dots1\#11\dots1\underline{\#})$
- Configuración final $(\text{FIN}, 11\dots1\underline{\#})$
- Solución:
 1. Movernos a la izqda una celda.
 2. Movernos hasta el # de separación y poner un 1.
 3. Movernos a la dcha hasta el # final y nos movemos a la izda una celda.
 4. Poner un #.
 5. Fin.

$MT = (Q, \Sigma, \delta, q_0)$

$Q = (q_0, q_1, q_2, q_3, q_4)$

$\Sigma = \{\#, 1\}$

El célebre código Enigma

Introducción

Los alemanes para asegurar que sus mensajes interceptados no fueran descifrados, la milicia germana hizo uso de varios dispositivos distintos durante la Segunda Guerra Mundial:

- La Fuerza Aérea y la Marina usaban una máquina llamada Enigma.
- El Ejército utilizaba la T52 la cual se conectaba a sus máquinas de teletipo.

La Enigma se usaba para cifrar en clave el código Morse. El SZ se usaba para enviar mensajes mediante teletipo a los diferentes cuarteles del ejército.

La Enigma

La máquina codificadora más famosa de la Alemania nazi fue inventada (en 1919) por un holandés: Hugo Alejandro Koch.

El ejército alemán introdujo algunos cambios en la Enigma inicial.

La versión militar de la Enigma constaba de 5 componentes variables:

1. Un tablero de conexiones que podía contener de 0 a 13 cables duales (es decir, de 2 conectores).
2. Tres rotores secuenciales, ordenados de izquierda a derecha, que conectaban 26 puntos de entrada a 26 puntos de salida, colocados en caras opuestas de un disco.
3. Veintiséis incisiones en la periferia de los rotores, las cuales permitían al operador especificar su posición inicial.
4. Un anillo movable en cada uno de los rotores, el cual asociaba un número (del anillo) con una letra del rotor que tenía a su izquierda.
5. Un sem rotor reflector (que realmente no se movía), que servía para asegurar que las entradas y salidas quedaran sobre los puntos de contacto adecuados.

El funcionamiento básico de la Enigma era que los rotores se encargaban de reemplazar una letra del mensaje por otra. Cada vez que se escribía una letra, el primer rotor giraba 1/26 de una revolución, de manera que la letra pudiera ser sustituida por otra, dependiendo de la posición inicial de la máquina y la forma en que los rotores estuvieran conectados. El segundo rotor sólo se movía cuando el primero hubiese rotado 26 veces y el tercero hacía lo propio cuando el segundo hubiese girado igual número de posiciones. Esto implicaba que la Enigma usaba un sistema polialfabético, porque la misma letra podía ser sustituida por varias letras distintas a lo largo de un mensaje. Por ejemplo, una 'A' podía ser codificada como una 'M' al principio de un mensaje y más adelante (en el mismo mensaje) ser codificada como una 'T'.

Habían ciertas características de la Enigma que facilitaban un poco la tarea de decodificación. Por ejemplo, las sustituciones que se realizaban eran tales que una letra nunca podía ser codificada consigo misma. Es decir, una 'A', nunca podía aparecer como 'A' en el mensaje en clave.

Los anillos móviles alrededor de los rotores también incrementaban la complejidad de la máquina. Su objetivo era asignar un número a cada posición del rotor (la cual a su vez correspondía a una letra), de manera que aunque se supiera cuál era la posición inicial de los rotores, el mensaje no podría descifrarse si no se conocía la posición física de los anillos.

En julio de 1939 los servicios de inteligencia de Inglaterra y Francia descubrieron que un grupo de criptógrafos polacos había estado decodificando desde 1932 los mensajes secretos que los alemanes transmitían con la Enigma.

Cuando los alemanes complicaron más el código de la Enigma en 1938, los polacos construyeron unas máquinas de relevadores llamadas "bombas", las cuales simulaban el movimiento de los rotores de la Enigma.

El equipo de criptógrafos británicos adoptaron la máquina polaca, perfeccionándola posteriormente. Una versión mejorada de las "bombas" fue diseñada por Alan Turing en 1940. La "bomba" inglesa medía unos 2.4 metros de alto y tenía unos 2.4 metros de diámetro en la base, la cual tenía la forma de una cerradura antigua.

Colossus : El Secreto Mejor Guardado por los ingleses durante la Segunda Guerra Mundial

Si la bomba atómica fue el secreto mejor guardado por los norteamericanos durante la Segunda Guerra Mundial, su equivalente en Inglaterra fue el *Colossus*, la primera computadora electrónica del mundo que se diseñó explícitamente para poder descifrar los mensajes secretos de los nazis.

La primera *Colossus* se puso en funcionamiento en diciembre de 1943. La máquina resolvió adecuadamente su primer problema en sólo 10 minutos.

Características principales

Algunas de las características más importantes de *Colossus* eran las siguientes:

- Usaba bulbos a gran escala y empleaba el sistema binario.
- Sus datos de entrada los leía de una cinta de papel perforada usando una lectora fotoeléctrica.
- Usaba circuitos de dos estados y sus operaciones eran controladas mediante los pulsos de su reloj interno, siendo posible hacerla operar a cualquier velocidad, lo cual era muy útil para probarla.
- Sus circuitos permitían efectuar operaciones Booleanas y efectuar operaciones aritméticas en binario.
- Sus funciones lógicas podían manejarse de manera preestablecida usando un tablero de interruptores, o podían seleccionarse de manera condicional usando relevadores telefónicos.
- Era totalmente automática.
- Tenía una memoria de cinco caracteres de cinco bits cada uno, los cuales se almacenaban en un registro especial.

- Su velocidad de operación era de 5,000 Hertz (ciclos por segundo).
- Medía 2.25 metros de alto, 3 metros de largo y 1.20 metros de ancho.
- Sus resultados se almacenaban temporalmente en relevadores para luego darles salida a través de una máquina de escribir eléctrica que funcionaba a una velocidad de 15 caracteres por segundo.
- Permitía saltos condicionales.
- No contaba con programas almacenados internamente y era, obviamente, una máquina diseñada explícitamente para tareas criptográficas.
- Internamente generaba cadenas de 501 bits.

📁 Programación primitiva

Los resultados producidos por *Colossus* no eran el texto final decodificado, sino más bien un mensaje intermedio que debía ser procesado a mano. Sin embargo, Irving John Good y Donald Michie descubrieron que efectuando ciertos cambios en las conexiones de la máquina mientras ésta estaba en operación, era posible que *Colossus* realizara la tarea que los criptógrafos efectuaban a mano. Este fue un descubrimiento muy importante y la técnica se incorporó de manera automática en la *Mark II Colossus*, completada el 1 de junio de 1944, sólo un mes después de haber sido encargada.

📁 Descendientes

La *Mark II Colossus* era cinco veces más rápida que su predecesora, pues usaba una memoria temporal implementada con registros de cinco etapas, además de operar en paralelo y realizar automáticamente la reutilización de información descubierta por Good y Michie.

La nueva versión de *Colossus* usaba 2,400 bulbos y era mucho más flexible que su predecesora. De hecho, se sabe que Geoffrey Timms demostró al final de la guerra que casi se podían efectuar multiplicaciones en base 10 con ella.

Se estima que hacia el final de la guerra habían al menos 10 máquinas *Colossus* en operación (todas ellas distintas) y varias más estaban produciéndose.

📁 Destino incierto

Aparentemente se destruyeron ocho de las 10 máquinas *Colossus* en 1946, por orden directa de Winston Churchill. Una más sobrevivió hasta los 1950s, y la última fue desmantelada en 1960 cuando todos los diagramas de sus circuitos y sus planos fueron quemados. Las razones no fueron sólo militares, sino también políticas, pues se sabe que hubo al menos un bombardeo alemán a una ciudad inglesa que pudo haberse evitado gracias a *Colossus*.

CONTRAINFORMATICA

A diferencia de virtualmente en las otras formas de guerra, no hay entradas forzadas en el espacio cibernético. Si los intrusos cibernéticos entran en un sistema lo hacen a través de caminos instalados en el propio sistema: algunos son pasajes y otros son problemas (es decir, pasajes indocumentados) que nunca se eliminaron.

En efecto, la protección existe. Muchos sistemas de información operan con varias capas: estas son maneras de separar los usuarios ilegítimos de los legítimos; cerraduras para impedir que usuarios legítimos tomen control deliberada o inadvertidamente de los sistemas de ordenadores, y dispositivos de seguridad para que incluso la usurpación del control no cree un peligro público.

Los intrusos cibernéticos, por su parte, primero deben engañar al sistema haciéndole creer que son usuarios legítimos (robando o adivinando una contraseña), y segundo, adquiriendo privilegios de control (con frecuencia explotando fallas endémicas) negados a la mayoría de los usuarios comunes. Con esos privilegios de "superusuario", los atacantes pueden eliminar archivos claves, escribir disparates en otros, o abrir una puerta oculta para volver a entrar después.

La mayor parte de los sistemas usan contraseñas para limitar la entrada, pero las contraseñas tienen muchos problemas bien conocidos: demasiadas de ellas son fáciles de adivinar; pueden ser robadas al pasar por las redes, y generalmente se las guarda en lugares esperados de una computadora servidora o anfitriona. Los métodos criptográficos como las firmas digitales disminuyen estos problemas (haciendo inservible capturar y repetir los mensajes de acceso). Las firmas digitales incluso ayudan a asegurar que todo cambio en un banco de datos o programa, una vez firmado electrónicamente, pueda ser rastreado a su originador, lo cual también es útil para el caso en que el atacante sea alguien de la propia firma que tiene privilegios de usuario.

Los sistemas operativos de los ordenadores y redes son vulnerables a los programas insertados por intrusos cibernéticos, como los virus (programas de ordenador que infectan a otros programas y hacen que a su vez infecten a otros programas más); caballos de Troya (programas de ordenador aparentemente útiles con trampas ocultas) y bombas lógicas (programas que permanecen letárgicos hasta que se los despierta).

Los sistemas también pueden ser puestos en peligro desde otros sistemas que ellos consideran de confianza. Se pueden tomar dos precauciones contra este peligro: reducir la lista de sistemas de confianza y limitar la cantidad de mensajes a los que reaccionará el sistema propio. Y una precaución final es desenchufarla. Como último recurso, muchos sistemas (como las plantas generadoras de energía nuclear) funcionan casi tan bien aunque no estén conectadas al mundo exterior.

Elementos esenciales

Cualquier estrategia que haga que nuestras Infraestructuras Críticas sean más fiables (resistentes) debe comprender tres elementos básicos: una mayor protección frente a las agresiones cibernéticas, la capacidad de detectar cuándo ocurre una agresión y la capacidad de responder y recuperarse cuando una agresión ha sido detectada.

La protección frente a la agresión cibernética se basa en la tecnología del cifrado de datos -- incluyendo las firmas codificadas digitalmente -- la cual proporciona servicios de autenticación, integridad, prevención de la posibilidad del repudio y privacidad y confidencialidad necesarios para garantizar la información. Quizá la mejor arma de protección contra la agresión cibernética sea la autenticación basada en la codificación digital que se emplea para dar acceso a la información. El cifrado se emplea en ordenadores, en los servidores y en todas las redes para asegurar que la información

referente a asuntos confidenciales de gobierno y de particulares se mantenga en esas condiciones. La tecnología del cifrado, que antaño fue patrimonio exclusivo de los gobiernos, se distribuye hoy libremente en el mercado y constituye un garantizador básico de la seguridad de información.

En cuanto al diagnóstico, detección y respuesta a la agresión cibernética, la tecnología no está tan avanzada ni es tan efectiva. Hoy día, Estados Unidos tiene muy poca capacidad de detectar o reconocer una agresión cibernética dirigida a las infraestructuras del gobierno o del sector privado, y todavía tiene menos capacidad de respuesta. La capacidad de identificar una agresión cibernética estratégica contra a uno o varios componentes de la infraestructura crítica, y responder de un modo apropiado, es claramente un tema de seguridad nacional impor tante.

ATAQUES DE COMANDO Y CONTROL: EXPLOTACIÓN DE LA INFORMÁTICA COMO ARMA OFENSIVA.

Podemos distinguir entre los siguientes tipos de guerra:

📁 Guerra Electrónica.

La guerra electrónica utiliza medios electrónicos para neutralizar los sistemas de mando y control enemigos, actuando sobre sus sistemas de comunicaciones y electrónicos, mientras que garantiza la integridad de sus propios sistemas. Este tipo de acciones existe desde que los militares comenzaron a utilizar el telégrafo, en 1850. Los equipos específicos de guerra electrónica comenzaron a surgir de manera eficiente y coordinada durante la Segunda Guerra Mundial, y constituyen, hoy, un componente común del arsenal de cualquier ejército.

📁 Ciberguerra.

El concepto de ciberguerra, si bien a veces es conocido de manera diferente con relación al concepto de guerra electrónica, puede ser considerado como parte íntegra de dicho concepto. Por lo tanto, la ciberguerra incluye la utilización de todas las herramientas disponibles al nivel de electrónica y de informática para derrumbar los sistemas electrónicos y de comunicaciones enemigos y mantener nuestros propios sistemas operacionales. Muchas de las acciones a desarrollarse en este campo aún no se encuentran definidas claramente a causa, en parte, del hecho de que hay equipos nuevos continuamente y que sólo recientemente es que los militares comenzaron a considerar este campo tecnológico como una nueva forma de guerra.

Algunos elementos de la ciberguerra aparecen aquí y allí de manera irregular y poco sistematizados, a medida que las oportunidades de su utilización van surgiendo. Los "cibersoldados" se encontrarán normalmente confinados a Centros de información de combate equipados con monitores, ordenadores y otros equipos de alta tecnología, mantenidos por técnicos especializados. Su misión consiste en garantizar que los comandantes reciben datos actualizados de la situación en el campo de batalla.

📁 Guerra de la Información.

1. Concepto.

Abarca todo aquello que se pueda hacer para proteger que nuestros sistemas de información no sean explotados, corrompidos o destruidos a la vez que, simultáneamente, se explotan, corrompen y destruyen los sistemas de información del enemigo.

2. Actividades Ofensivas de la Guerra de la Información.

- Obtener información del adversario sin que éste se dé cuenta.
- Alterar o dañar la información ya obtenida y almacenada por el adversario con el propósito de engañarlo y hacer que éste confíe en la información que utiliza aún cuando ésta sea falsa.
- Desinformar al adversario proporcionando a sus medios de búsqueda información totalmente falsa o parte de información verdadera cuidadosamente seleccionada para lograr un propósito específico.
- Destruir físicamente información, procesos basados en información y sistemas de información del adversario. Esta actividad resulta bastante amplia ya que comprende desde el borrado de un disco hasta la destrucción de un centro de mando y control.
- Negación de los elementos o servicios que requieren para funcionar los procesos basados en información y los sistemas de información.

Espionaje.

La obtención encubierta de información del adversario ha sido uno de los objetivos principales de las Operaciones de Inteligencia, específicamente por medio del espionaje. Permite a quien lo gesta tener conocimiento con anterioridad de las intenciones y capacidades del adversario y a la vez saber cuan profundo es su conocimiento de las intenciones o capacidades propias con el consiguiente beneficio en la toma de decisiones.

Sabotaje.

A diferencia del espionaje, la forma de materializar el sabotaje como Operación de Inteligencia en el contexto de la GI podría sufrir varias transformaciones, especialmente debido a las posibilidades que las herramientas informáticas ofrecen hoy en día para ingresar a sistemas de información y alterar o destruir en forma encubierta los datos almacenados en ellos. Pero no sólo la información y los sistemas de información serán objetivos del sabotaje en la GI sino que también todos los procesos o sistemas que de alguna u otra forma ayudan a sostener la malla de información de un país. Es así como, por ejemplo, los altamente automatizados sistemas de producción y control de energía eléctrica se han transformado en un objetivo tan prioritario como la misma información en el campo de batalla de la GI.

ECHELON

Echelon tiene la capacidad de interceptar todos los días la cifra de tres mil millones de comunicaciones (cerca del 90% del tráfico de Internet) incluyendo llamadas telefónicas, mensajes de correo electrónico, descargas de Internet, transmisiones por satélite, etc.

El sistema recoge estas transmisiones, las clasifica y resume la información mediante programas de Inteligencia Artificial. ¿Cómo lleva a cabo Echelon sus tareas rutinarias de espionaje? Echelon cuenta con superordenadores, denominados Diccionarios, que son capaces de almacenar en un amplio banco de datos, información relativa a nombres, direcciones, números de teléfono, etc.

El proceso es el siguiente: cuando un satélite detecta una comunicación relevante, el mensaje se selecciona y se envía a los centros especializados de la NSA y del GCHQ para su archivo. EL filtrado de las conversaciones se realiza por la preselección de los números de teléfono y de las identidades fónicas (la huella vocal individual). Además de esto Echelon utiliza lo que denominan “bosques semánticos”.

Este proyecto aglutina los servicios secretos y policía de los EE.UU y de Europa con objeto de coordinar una fórmula que les permita “espíar” las comunicaciones por Internet y el teléfono sin ningún tipo de control. En esta dimensión entra el problema de la captación de datos personales. Enfopol permite registrar los números marcados después de haber cortado la llamada, direcciones IP, nombres de usuarios y contraseñas, números de cuenta, números PIN, dirección de correo electrónico, números de teléfono, nombre completo, dirección, número de cuenta, etc.