

Ciberterrorismo I

Espionaje En Las Redes De Ordenadores

Grupo 2

Andy Xavier Gómez Gálvez	0510-2000-00607
Erick Sebastián Moncada Rubí	0801-2000-17208
Josué Isaac Menas Mejía Hernández	0801-2001-07890
German David Ordoñez Gómez	0801-2001-21597
Lesnin Roberto Ramírez Castellanos	0801-2000-11557

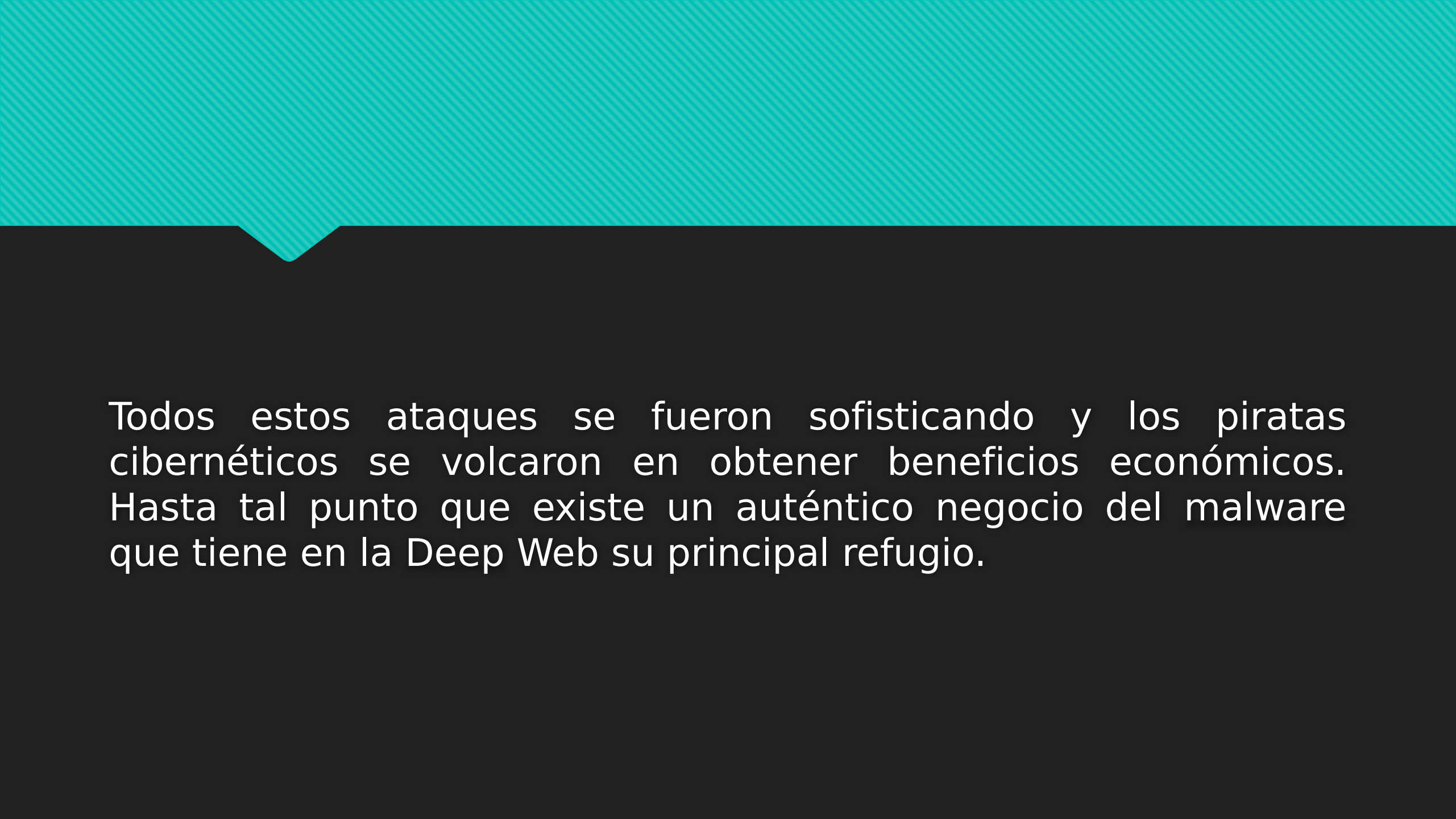
¿QUÉ ES UN CIBERATAQUE?

Un ataque informático consiste en la agresión a una empresa o a un individuo mediante herramientas informáticas con un objetivo de obtener beneficios de forma ilegal, infligiéndole un daño ya sea un robo de información confidencial o de propiedad industrial.



¿CÓMO HAN EVOLUCIONADO LOS ATAQUES A LO LARGO DE LA HISTORIA?

En un principio, los ataques provenían hackers o jóvenes que querían notoriedad y prestigio. No resultaban especialmente dañinos teniendo en cuenta que la difusión de las redes de equipos no era muy grande y por tanto la capacidad de contagio resultaba limitada.



Todos estos ataques se fueron sofisticando y los piratas cibernéticos se volcaron en obtener beneficios económicos. Hasta tal punto que existe un auténtico negocio del malware que tiene en la Deep Web su principal refugio.

¿QUÉ HACEN LAS EMPRESAS Y LOS ORGANISMOS PARA PROTEGERSE DE LA INSEGURIDAD INFORMÁTICA?

Algunos proveedores de ciberseguridad utilizan mapas en tiempo real para conocer al segundo los ataques que se están realizando, como es el caso de Kaspersky que muestra las detecciones que se están produciendo a nivel planetario.



PAÍSES DONDE MAS OCURRE CIBERTERRORISMO

Según Riptech, empresa de seguridad informática creada en 1998 por antiguos expertos del departamento de Defensa de EE UU

Cuba, Irán, Sudán, Irak, Libia, Corea del Norte y Siria,. Aunque sólo los tres primeros han dejado huellas indiscutibles de ataques informáticos efectuados desde su territorio.

Se da el caso, además, de que 9 de cada 10 sabotajes correspondientes a dichos países proceden de Irán. El 10% restante se originó, a partes iguales, entre el país caribeño, Cuba, y el africano Sudán.

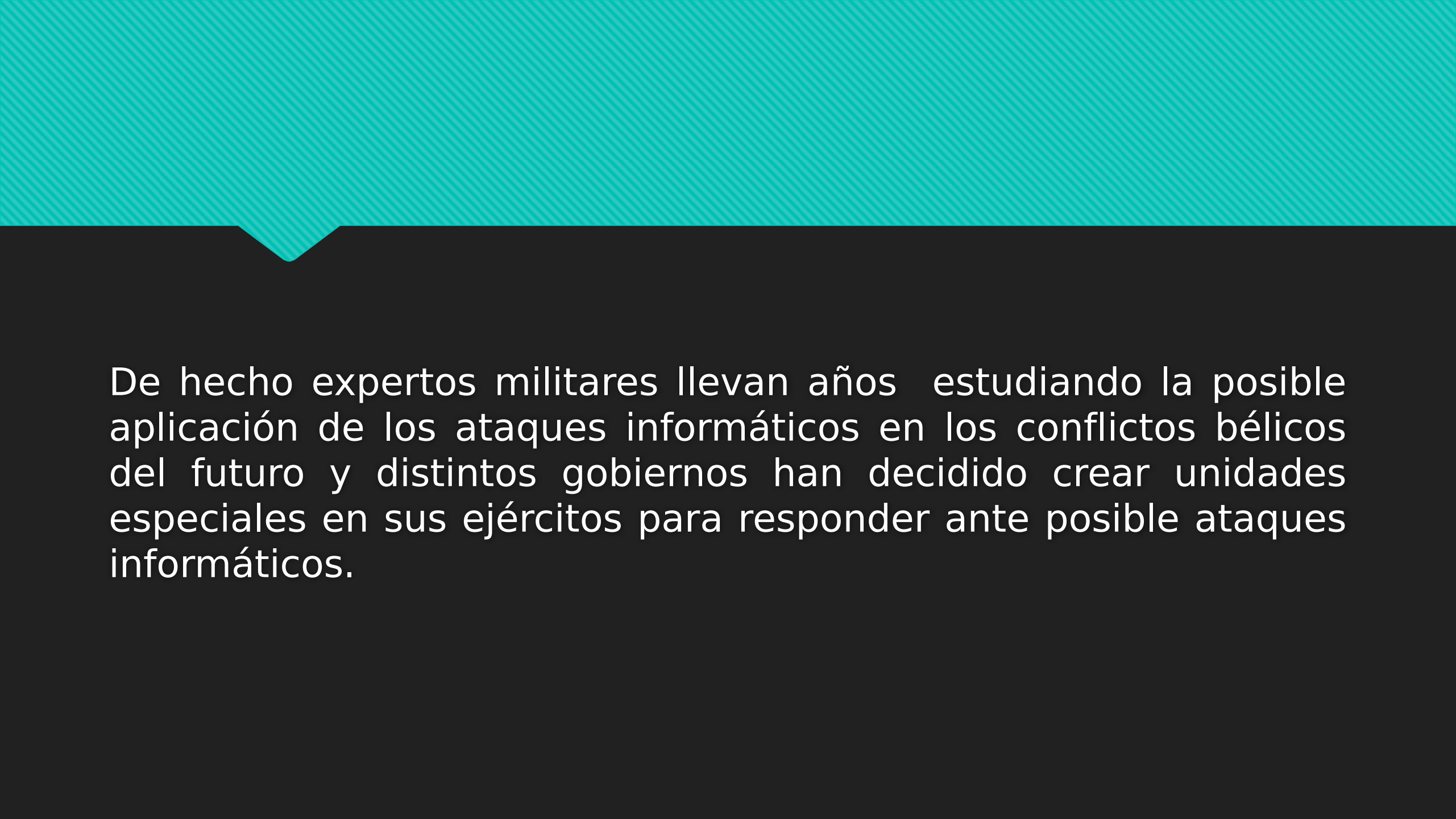
Entre los países que presentan mayor actividad como emisores de ataques informáticos son, de mayor a menor, Kuwait, Pakistán, Egipto e Indonesia. La suma de sabotajes desde naciones integradas en una y otra lista produce un porcentaje inferior al 1% respecto al total de ataques confirmados en todo el mundo.

¿Cuántos ciberataques hay en el mundo?

Según IDC Reseach, El mismo informe señala que cada día se producen en el mundo 350.000 ataques de malware.

LA AMENAZA DEL CIBERTERRORISMO Y DE LAS GUERRAS INFORMÁTICAS

La sociedades avanzadas tienen una dependencia cada vez mayor de los sistemas informáticos para el control de muchos procesos y actividades cotidianas, se podría colapsar el funcionamiento de un país desarrollado si se dañasen algunos de sus principales redes y sistemas informáticos.



De hecho expertos militares llevan años estudiando la posible aplicación de los ataques informáticos en los conflictos bélicos del futuro y distintos gobiernos han decidido crear unidades especiales en sus ejércitos para responder ante posible ataques informáticos.

POSIBLES CONSECUENCIAS DE UNA GUERRA INFORMÁTICA

- ❖ Corte del suministro eléctrico y posible descontrol de centrales nucleares, centrales hidroeléctricas y térmicas.
- ❖ Colapso total de las redes telefónicas y los sistemas de comunicaciones.
- ❖ Desarrollo de ataques específicos contra los sistemas de comunicaciones militares.



- ❖ Caos financiero
- ❖ Intervención del control del tráfico aéreo y ferroviario
- ❖ Ataques informáticos de todo tipo protagonizado por virus, programados y controlados de forma remota para activarse en el momento adecuado
- ❖ Destrucción de grandes bases estatales vitales para el funcionamiento del país.
- ❖ Equipos electrónicos militares no protegidos y silenciar a las principales emisoras de radio y televisión.

ALGUNOS EJEMPLOS DE LA VIDA REAL DE CIBERTERRORISMO

En agosto de 2008 un fallo informático en la agencia federal de aviación (FAA) de estados unidos provocaba un colapso del trafico en todo el país.

En 2009 una investigación llevada a cabo en Toronto revelaba que una red de espionaje informático había logrado penetrar en los ordenadores de gobierno de las embajadas de hasta 103 países.



ESPIONAJES EN LAS REDES DE ORDENADORES

El polémico chip “Clipper y el papel de la” NSA

A principios de los años noventa surgía la polémica en Estados Unidos por la intención del gobierno de es país de intervenir en todo tipo de comunicaciones a través de redes telefónicas y de ordenadores. Así, en 1994 la Administración Clinton aprobó el Escrowed Encryption Standard que contemplaba el desarrollo de productos con la característica de “key-escrow”, para facilitar el descifrado de las comunicaciones por parte de organismos del gobierno (como la CIA o el FBI).

CARNIVORE

CARNIVORE es un polémico programa desarrollado en el año 2000 por el FBI en Estados Unidos para interceptar y leer mensajes de correo electrónico y otras comunicaciones entre presuntos criminales, espías y terroristas, contando para ello con la colaboración de los operadores de redes de telecomunicaciones.

Desde entonces este costoso programa (el proyecto tuvo un coste superior a 170 millones de dólares) fue utilizado de forma importante a partir de los atentados de 11-S en Estados Unidos.

Sin embargo, en enero de 2005 el FBI anunciaba su intención de desechar este programa y reemplazarlo por otras soluciones comerciales convencionales que resultaban mucho más económicas.

En la actualidad la investigación también sesenta en la interpretación de las conversaciones mediante telefonía IP (transmisión de voz a través de la propia Internet).

ECHELON

ECHELON es una red de espionaje electrónico creada en los años cincuenta por la Agencia Nacional de Seguridad norteamericana (NSA), contando con la colaboración de Gran Bretaña, Australia y Nueva Zelanda.

ECHELON es un sistema militar de espionaje de todo tipo de comunicaciones electromagnéticas, con capacidad para interceptar llamadas de teléfono (incluso a teléfonos móviles con el sistema GSM, que emplea algoritmos de cifrado), transmisiones por Internet, envíos de fax y télex, transmisión de datos y de llamadas vía satélite, etc.

