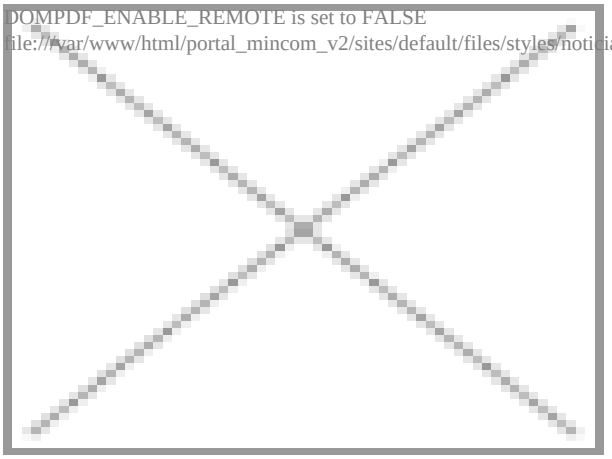
DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/all/themes/mincom/logo.png

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/default/files/styles/noticias/public/cia.png


Source:
Tomado de CubaSí

Por estos días se ha dado a conocer informaciones sobre los programas de espionaje masivo de la CIA y la Agencia de Seguridad Nacional estadounidense (NSA), también del crecimiento de los ataques informáticos a sitios de organismos políticos y de masas, de la administración y estudiantiles de Cuba.

Un informe de investigación publicado recientemente por el Centro Nacional de Tratamiento de Emergencias de Virus Informáticos de China, revela como Estados Unidos ha desarrollado una estrategia ciberespacial significativamente más ofensiva, ha planeado y organizado un gran número de “revoluciones de colores” en todo el mundo, con la ayuda de una poderosa tecnología de redes y comunicaciones.

Estados Unidos encabeza los países que han desarrollado complejos sistemas de exploración informática globales para alcanzar una supremacía en la adquisición de información estratégica en las esferas militar, política e industrial. Los programas PRISM, Eshelon, Carnivore, NarusInsight, Turbulence, CO-TRAVELER, Dropmire, X-Keyscore) así lo prueban.

Sobre estas cuestiones estaremos hablando con Daniel Ramos Fernández, director de negocios digitales de la Empresa de Telecomunicaciones de Cuba (ETECSA) y experto en sistemas informáticos y ciberseguridad.

DRF: Ya en el año 2017 estos sistemas eran capaces de interceptar diariamente en todo el mundo, más de 1 700 millones de llamadas telefónicas y correos electrónicos, acceder a información de más de 5 000 millones de teléfonos móviles y conocer la ubicación y movimientos de sus propietarios.

Dentro de los programas filtrados en el 2013 por Edward Snowden, ex funcionario de la CIA y analista de la empresa privada de consultoría de inteligencia Booz Allen Hamilton estaba el PRISM, que autorizaba a la NSA a tener acceso no autorizado a todos los datos privados almacenados en los servidores de grandes empresas de internet como Microsoft, Google, Apple, Facebook, Skype, entre otras. Incluía los correos electrónicos, chats, fotografías, videos, transferencia de archivos y otros datos y metadatos.

A partir de la década de 1960 el gobierno estadounidense y sus agencias de inteligencia tejieron una red de más de 120 emisoras de radio que abarcó a varios países, con el objetivo de destruir a la Revolución Cubana, agredir la soberanía nacional y promover la subversión contra el orden constitucional que se diera libre y soberanamente nuestro pueblo.

OPS: El 9 de septiembre de 2001, dos días antes del ataque terrorista a las torres gemelas en New York, Cuba se convierte en el primer Estado acusado de planear ataques cibernéticos contra Estados Unidos, cuando en la audiencia del Comité selecto del Senado sobre Inteligencia, que trató el tema de “la amenaza mundial”, el entonces director de la Agencia de Inteligencia de Defensa, Almirante Thomas R. Wilson,

identificó a Cuba como un posible país “ciberatacante”. También en febrero de 2006 el Departamento de Estado, encabezado por Condolezza Rice, creó el Grupo de Tarea para la Libertad Global de la Red, que debía concentrarse en monitorear especialmente a China, Irán y Cuba. Posteriormente se ejecutaron diversas operaciones anticubanas utilizando las tecnologías de la información y la comunicación.

DRF: Diversas operaciones subversivas desarrolladas por el gobierno yanqui y sus agencias de inteligencia se canalizaron a través de organizaciones, fundaciones, compañías profesionales internacionales y personas naturales. Se destacan Zunzuneo, que bajo la apariencia de una red social inocente, encubrió una operación secreta financiada y dirigida por la Usaid. En el 2012 captó más de 40 mil suscriptores cubanos que desconocían, hasta que fue denunciado por ETECSA, que detrás del servicio había contratistas que recopilaban información privada con fines políticos.

Más detalles https://bit.ly/41B3bkA [1]

Links
[1] https://bit.ly/41B3bkA