Espionaje (Enemigo público)

Veloza Hernández Luis Eduardo
luisvelozah@gmail.com
Universidad Piloto de Colombia

Resumen—Desde hace algunas décadas, el internet viene siendo el canal de conexión de una infinidad de redes que funcionan como el motor de los aspectos básicos de la vida. De ahí que la economía y la seguridad del universo estén sujetas a las TIC.

Como producto de lo anterior y siendo el centro de atención y discusión de este documento, aparece el espionaje cibernético o ciber-espionaje que irrumpió, tomó vida e importancia, y se convirtió en parte vital del oficio político gubernamental.

Con relación a la enunciación previa, dentro del espionaje cibernético se practican dinámicas en las que los integrantes de los gobiernos actúan por medio de la red como guardianes que vigilan con el propósito de detectar cualquier ataque que pueda generarse contra su gobierno, o para beneficiarse y tomar ventaja de cualquier vulnerabilidad que presenten los gobiernos de las naciones externas.

***Abstract*—some time ago, internet has been the connection channel of an infinity of networks which work as the engine of the life basic aspects. That is why the economy and security of the universe are up to the information technologies and communication.**

As a result of the previous statement and being this document the focus of attention and discussion, appears the cyber espionage that took life and importance. Besides, this, the cyber espionage became in a governmental work vital part.

According to the enunciation above, into the cyber espionage some dynamics are practiced, the ones who practice these dynamics, the same which belong to the different governments, act through the network as keepers that watch over with the purpose of detecting any attack that goes against their government or, to take advantage of any vulnerability of governments by external nations.

Índice de Términos—Tics, espionaje-ciber-espionaje, nación, gobierno, comunicación, ataque, delito informático.

I. INTRODUCCIÓN

En el siguiente documento se hace un breve estudio tanto a la llegada y funcionamiento del espionaje cibernético; la conexión que existe entre este y los gobiernos del mundo, pero más enfáticamente, el estudio se enfoca en la relación que hay entre ciber-espionaje-Estados unidos. Se intentan identificar las causas y consecuencias que dicha relación ocasiona y cómo eso afecta al mundo entero.

II. ESPIONAJE ENTRE PAÍSES

La historia de la humanidad ha sufrido diferentes cambios causados por fenómenos que con su aparición resultan caracterizarse como factores facilitadores de los procesos que modulan; avanzan y/o retrasan el desarrollo de la sociedad en general.

Uno de los factores que se ha convertido en la vitalidad del mundo de la evolución es la incursión de la tecnología, cuya participación y utilidad en todos los aspectos de la vida de las personas (económicos, personales, sociales y gubernamentales.) le otorgan una soberanía tal que en la actualidad parece imposible no contar con la ayuda tecnológica o prescindir de los servicios la misma, si lo que se desea es incrementar las tareas y su efectividad teniendo en cuenta el factor tiempo y la competitividad de nuestros días.

Aunque la tecnología según expertos ha sido creada quizás, sólo con fines positivos y de crecimiento, esta también ha generado inconsistencias y alteraciones que se convierten en delito informático, el cual está relacionado particularmente con el espionaje de datos; un fenómeno que afecta a muchas empresas, multinacionales, y, en igual o mayor medida, a los países.

El espionaje de datos es un problema que ha causado cambios diplomáticos, pero también, ha fomentado la inversión de significativas cantidades de dinero en el diseño e implementación de nuevas prácticas que permitan seguridad a la información privada, confidencial y clasificada que forma parte de la seguridad de un país.

Adicionalmente, con el desarrollo y la sofisticación tecnológica, el espionaje cibernético industrial y gubernamental, también ha llegado a un más alto nivel de complejidad y ha obtenido mayores alcances.

Cabe mencionar que Estados Unidos ha sido un país que ha sufrido fuertes ataques a la integridad y seguridad de sus datos, de la información que pertenece al país. Ahora bien, esos ataques le han servido como fuentes de estímulo para la realización e invención de dispositivos, métodos y organizaciones o grupos especializados en la formación e implementación de nuevas y mejores políticas, prácticas y leyes de seguridad.

Uno de los ataques al gobierno norteamericano que ha estimulado a los representantes políticos del país a buscar alternativas que ayuden y prevengan eventualidades futuras, es el caso que se presentó en el año 1971 al FBI: *Federal Bureau of Investigation u Oficina legal de investigación* (grupo de investigación judicial de los Estados unidos).

El robo de la documentación que en ese entonces allí se tenía; robo que fue ejecutado por un grupo de activistas estadounidenses no simpatizantes con la guerra de Vietnam, quienes querían como primera medida:

Comprobar y asimismo, demostrar por medio de los documentos obtenidos, que dicho grupo de investigación y seguimiento judicial norteamericano tenía como objetivo de asedio y persecución a los manifestantes izquierdistas o "contrapolíticos" de la época. [1]

El suceso anterior nos revela la importancia de crear estrategias acompañadas de dispositivos tecnológicos que permitan impedir la manipulación de datos que son de uso y conocimiento exclusivo, archivos que si es transgredido el límite del personal a su acceso, pueden causar inconvenientes al funcionamiento de una familia, compañía, y en este caso particular, a la administración de una nación.

Así las cosas, hablando en términos de seguridad y de desarrollo tecnológico, y para prevenir hecatombes, gracias al robo de 1971, se vislumbra y

se revela cuan relevante, necesario e indispensable es crear y poner en marcha un protocolo que tenga como elementos inherentes:
La ejecución de una serie de estrategias preventivas que mantengan resguardada la información de los interesados, y de igual manera, provocar la invención del tipo de herramientas o maquinas tecnológicas diseñadas y aptas para la consolidación de tal protocolo.

En efecto, el evento surgido en la omnipresente y más poderosa nación, dio lugar a la tentativa de incrementar la seguridad tanto del material informativo de valor como de las dinámicas que se presentan en las oficinas del gobierno norteamericano.

Es por eso que surge la creación y participación de la Agencia De seguridad Nacional - National Security Agency: agencia de inteligencia que trabaja en función del gobierno estadounidense y se encarga de todos los procesos relacionados con la seguridad de la información.

La NSA se convierte entonces en el antídoto para los problemas de quienes mantienen la jefatura de los Estados Unidos. No obstante, con el paso del tiempo, la agencia de seguridad también llega a ser el veneno y yugo que deja como producto la zozobra y el malestar de todo aquel ser que viva y haya nacido bajo el seno, o pueda tener cualquier atractivo para los Estados Unidos de Norteamérica.

Teniendo como estrategia principal de desempeño laboral, la NSA concreta sus tareas haciendo uso del método de intercepción de datos de la población. Pero para interceptar la información, este organismo emplea diferentes caminos.

Como ente común para capturar, recolectar y almacenar datos, la Agencia**,** debido a que cuenta con la tecnología suficiente, con ayuda de esa, invade la vida y la privacidad de la ciudadanía capturando masivamente las comunicaciones telefónicas y electrónicas tanto en Estados Unidos como en diferentes países del mundo que puedan estar relacionados no necesariamente con los ataques, sino que puedan brindar información importante para la nación Estadounidense.

El diario "*la voz de América"* publica una noticia que hace referencia y soporta lo que anteriormente se mencionó. Entonces, el articulo noticiario nos cuenta que el actual presidente de Estados Unidos Barack Obama, si bien dice que es necesario conservar ciertas dinámicas espiratorias, también, decide poner límites al espionaje de la Agencia Nacional de Seguridad (NSA) por los excesos a los que esta, la NSA ha llegado. [1]

Igualmente se ha evidenciado que las cabezas titulares del país anglosajón han sabido sacar provecho del avance que han adquirido en el campo del espionaje cibernético y de las vulnerabilidades con las que cuentan otros gobiernos. De esta manera, han hecho del país el intruso más peligroso

y osado en espiar y capturar información tanto de los países vecinos de América latina como del territorio europeo.

Ahora bien, según lo analizado, el objetivo de EE.UU que antes era prevenir y cuidar su información, sin embargo, yendo más allá del objetivo principal, el propósito hoy por hoy, es capturar datos que le puedan servir para mejorar e ir uno o muchos pasos más adelante en cuanto a los aspectos tecnológicos, económicos, políticos e industriales de la nación con relación a las otras potencias.

Los gobernadores de los países afectados por la manera de operar de ·Estados Unidos, siendo conocedores de las invasiones y movimientos ilícitos estadounidenses, se han manifestado dando a conocer su indignación.

Una muestra de ello es el caso de la presidenta de Brasil, quien el año pasado decidió cancelar una visita que tenía programada al presidente Obama argumentado la ofensa que este le causa al espiar su correo. La gobernadora añadió que ese tipo de acciones no se le hacen a un país amigo. [2]

En consonancia con todo lo previamente descrito, cabe añadir más datos que prueban la activa participación de América del Norte en situaciones y proyectos de espionaje cibernético, haciendo partícipes a diferentes países del mundo entero.

En los años 70, más exactamente en 1977, surge la creación de una organización denominada la red *ECHELON* o *la Gran Oreja;* conformada por Estados unidos en acompañamiento de otras naciones de habla inglesa como Canadá, Reino Unido, Australia y Nueva Zelanda.

La red ECHELON es entonces "un entramado de antenas, estaciones de escucha, radares y satélites, apoyados por submarinos y aviones espía, unidos todos esos elementos a través de bases terrestres, y cuyo objetivo es espiar las comunicaciones mundiales, comunicaciones por medio de correos electrónicos, faxes, comunicaciones por cable, por satélite, radio y conversaciones telefónicas, *teóricamente*, para luchar contra el terrorismo internacional y el tráfico de drogas.
Es claro que el principal precursor del fenómeno del ciber-espionaje es el país norteamericano. Sin embargo, Colombia no siendo un país con significativos avances tecnológicos ni prácticas relacionadas con el espionaje o temas similares, siguiendo el ejemplo de Estados Unidos, se ha interesado y más aún, ha sido blanco de ejecución de intercepción ilícita de datos e información.

En el año 2009, el Departamento Administrativo de Seguridad de Colombia fue protagonista de los diarios y noticieros del país porque según esas fuentes, este, había sido responsable de "chuzar" ilegalmente conversaciones o comunicaciones de personajes políticos como magistrados de la Corte Suprema de Justicia, integrantes de partidos de

oposición, miembros de ONG, entidades internacionales de derechos humanos y periodistas. [4]

III. CONCLUSIONES

Analizando las situaciones anteriores, la transgresión de la privacidad y el uso de métodos para adquirir sin algún permiso información privada, buscando concordancias y discrepancias entre los diferentes sucesos relacionados con el tema, se puede concluir que USA ha sido un actor importante en la historia del espionaje y que sus manifestaciones han llegado a tan altos niveles que ya no sólo ocupan el territorio del país en mención, sino que también han desbordado los límites geográficos, de manera que ha llegado a involucrarse en la privacidad de los diferentes países del mundo. Además, ha sido tan repetitivo en sus acciones espiatorias que no sólo ha "violado" la integridad de otros gobiernos, sino que, de igual manera, ha influenciado a los estados externos a practicar las mismas formas de espionaje y adquisición arbitraria de información.

IV. REFERENCIAS

[1]. Press, T. A. (08 de Enero de 2014). UnivisionNoticias. Retrieved 10 de Enero de 2014 from UnivisionNoticias: http://noticias.univision.com/article/1792086/2014-01-08/estados-unidos/noticias/revelan-robo-de-documentos-al-fbi-que-destapo-espionaje-en-1941

[2]. Montaner, C. A. (21 de Septiembre de 2013). El blog de Montaner. Retrieved 13 de Enero de 2014 from El blog de Montaner: http://www.elblogdemontaner.com/por-que-estados-unidos-espia-brasil/

[3]. Website, E. D. (14 de Julio de 2003). bibliotecapleyades. Retrieved 15 de Enero de 2014 from bibliotecapleyades: http://www.bibliotecapleyades.net/ciencia/echelon02.html

[4]. Redacción, V. d. (17 de Enero de 2014). Voz de América . Retrieved 20 de Enero de 2014 from Voz de América: http://www.voanoticias.com/content/obama-ordena-limites-recoleccion-datos-nsa-espionaje-espias/1832343.html

Autores
Ingeniero de sistemas de la Universidad Autónoma de Colombia