Guerra por el Ciberespacio

Paola Andrea Zárate Luna
Especialización en Seguridad Informática, Universidad Piloto de Colombia
Bogotá, Colombia
Paz_45@hotmail.com

ABSTRACT

Day to day progress and acceptance of technologies in all countries regardless of social status, contributes to the cultural development of citizens, however the gap by the lack of education in areas of security and poor criminalized regulations for cybercrime allowed to expose and stop outdoor for free disposal personal information, resources, platforms and critical infrastructure of companies and governments, which may lead to a not very distant computer war. It is no longer enough to turn on a computer now know digital citizens will have to acquire knowledge's and skills to fight against cyber enemies.

Who has the information has the power…

David Hume

I. INTRODUCCIÓN

La evolución de las plataformas tecnológicas mundiales ha convertido el contexto de las guerras ocurridas años atrás, en guerras cibernéticas, pasando por el ámbito militar y tomando un nuevo rumbo en el conflicto internacional que enfrentan los Estados como consecuencia de dicha transformación. El nuevo dominio sobre el cual ejercen soberanía los gobiernos incluyendo el Colombiano es el ciberespacio; termino comúnmente utilizado por los cibernautas, para referirse a ese espacio virtual con diferentes instrumentos, que conforman una infraestructura tecnológica incluyendo internet, información y comunicaciones, desapareciendo las barreras de tiempo y lugar, siendo intangible y brindando ahora a los usuarios la oportunidad de adquirir herramientas de inteligencia digital colectiva.

II. PAÍS DE CIBERSEGURIDAD

El Ciberespacio se ha convertido en el arma de comunicaciones más peligrosa y poderosa que podría llegar a utilizar cualquier pirata informático sin mucha experiencia, en contra de un país que no se encuentra a la vanguardia en el ámbito de las tecnologías, o para quienes aún no dimensionan el valor de su información; convirtiéndose este entorno en un factor determinante al tener fuertes connotaciones futuristas para los gobiernos en aspectos como la economía, la política, la industria, el comercio y el nivel cultural de miles de ciudadanos de los diferentes países y continentes del mundo. [1]

La gran aceptación social de la tecnología ha desembocado en el desarrollo de aptitudes y actitudes de los ciudadanos colombianos quienes deben asumir nuevos comportamientos como requisitos de supervivencia y desarrollar competencias tecnológicas que les permitan no solo manipular adecuadamente los diferentes servicios y entornos virtuales de los medios tecnológicos sino también asumir una cultura cívica de seguridad de la información frente al uso racional y seguro de las tecnologías para evitar ser víctimas de fraudes y delitos informáticos.

El aumento progresivo y sosegado de la conectividad impulsada por el mismo gobierno Colombiano en términos de acceso, cobertura y velocidad (MinTic) ha desbocado un acrecentamiento elevado del cambio de la forma de presentar el portafolio de los servicios para los Colombianos al pasar de lo presencial a lo virtual, lo cual ha facilitado la aceptación e influencia social y cultural de un universo virtual.

Las últimas cifras arrojadas por estudios realizados a finales del año 2012 por el Ministerio de las Tics, muestra cómo ha evolucionado la tendencia del uso de internet en los hogares Colombianos; siendo el aumento más significativo para los estratos bajos: 1 y 2, demostrando que el 54% de los colombianos usan Internet. [2]

Por otra parte solo hasta el año 2009 con la ley 1273 del 05 de Enero el Congreso de la República de Colombia tiene por primera vez, un gran acercamiento con implicación penal, la ley "de la protección de la información y de los datos", adicionándose los artículos 269A "Acceso abusivo a un sistema informático", 269B "Obstaculización ilegítima de sistema informático o red de telecomunicación", 269C "Interceptación de datos informáticos", 269D "Daño Informático", 269E "Uso de software malicioso", 269F "Violación de datos personales", 269G "Suplantación de sitios web para capturar datos personales", 269H "Circunstancias de agravación punitiva:…", 269I "Hurto por medios informáticos y semejantes" y 269J "Transferencia no consentida de activos", promulga claramente la preservación de los sistemas de información y las comunicaciones y tipifica como delitos informáticos conductas que incurran en faltas a los artículos mencionados.

Dos años más tarde, el Ministerio de Defensa preocupado por el desarrollo tecnológico y las rápidas e innovadoras técnicas de los delincuentes al encontrar diferentes formas para la realización de fraudes; crea el Grupo Colcert una entidad interinstitucional cuyo objetivo se encuentra enfocado a crear protocolos para la seguridad de la información y tratar temas de ciberseguridad

participando en simulacros de ataques a infraestructuras críticas nacionales. El Colcert ha logrado posicionarse como uno de los mejor grupos de Ciberseguridad de América, hechos demostrados también en los pasados juegos cibernéticos regionales (Octubre de 2013); donde competidos de varios países participaron en una simulación de crisis por un ciber ataque a una Planta de Tratamiento de Agua, donde se había perdido el control de los servidores. El equipo Colombiano logro recuperar el control del mayor número de servidores, y arreglar los problemas de seguridad. [3]

III. Estadísticas De Ciberataques

De acuerdo a la emisión del día 9 de Mayo de 2012, del diario El Espectador, en su apartado de Tecnología, Colombia se posiciona como el tercer país de América Latina con más ataques cibernéticos de acuerdo al informe anual de Symantec, siendo el crecimiento tecnológico y el desarrollo en móviles la principal causa de exposición de grandes, medianas y pequeñas compañías, incrementándose los ataques en un 81% para el año 2011.

Según un informe del Registro de Direcciones de Internet para América Latina y Caribe (LACNIC), los fraudes por internet representan pérdidas anuales por unos US$93 mil millones y afectan a unos 2.500 bancos que operan en la región.

Otras páginas de eventos de seguridad informática http://zone-h.org muestran estadísticas del incremento para el año 2011 siendo este uno de los más altos, con 3006 notificaciones de ataques, mientras que para los años 2012 y 2013 se visualiza una variación debido a los pocos mecanismos de protección que empiezan a implementar las grandes y medianas compañías.

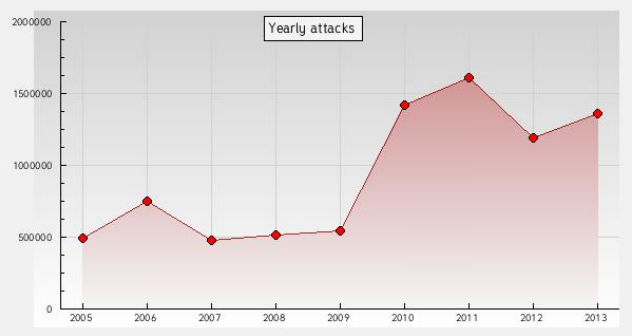

Fig. 1 Crecimiento CiberAtaques Anuales tomado de http://www. Zona-h.org

Por otra parte Karpesky Lab informó que su análisis sobre la naturaleza del delito cibernético en América Latina, que examina los primeros nueve meses de 2013, reveló que las computadoras de un 35% de usuarios en la región fueron atacadas por lo menos una vez mientras navega por la web.[4]

De acuerdo al reporte emitido por Norton del año 2013, los cibercriminales emplean ataques sofisticados que les permiten elevar la cantidad de ganancias y dinero obtenido por cada ataque, dichos hallazgos encontrados en Colombia apuntan que: [5]

- El 64% de los usuarios adultos ha experimentado algún crimen cibernético.
- El 64% de los colombianos usa sus dispositivos móviles para trabajar.
- En los últimos 12 meses el costo total del crimen cibernético en el país fue de 873 mil 466 millones de pesos.
- En el último año, 6 millones de personas han sido víctimas de cibercrimen.
- El 42% de los usuarios de Smartphone ha experimentado algún delito cibernético en los últimos 12 meses.

A menudo suele verse el incremento de la tecnología ligado con un grave desconocimiento de seguridad en comunicaciones, ya que la mayoría no se preocupa por tomar precauciones necesarias como inscripción de datos, contraseñas seguras, software de antivirus o protección del a información, políticas para salvaguardar la información, entre otras.

Algunas empresas de seguridad como McAfee también advierten en su boletín "Needle in a data risk: the rise of big security data"que solo el 35% de 500 compañías toman precauciones para identificar y controlar un ciberataque. En la siguiente grafica se puede visualizar cómo afecta directamente la privacidad de la información en la economía de las compañías independientemente de cual sea su razón social:

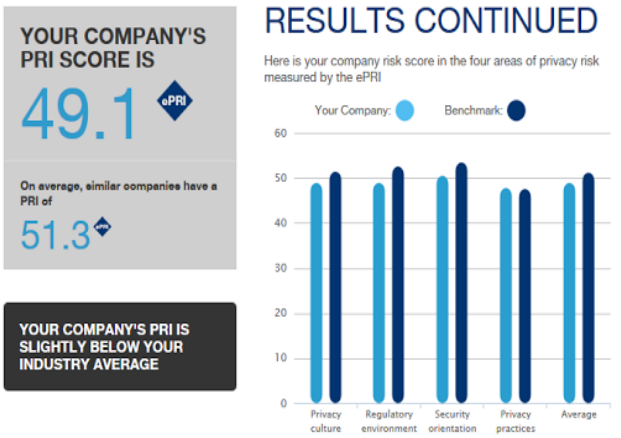

Fig. 2 Índice de crecimiento del riesgo de privacidad por CiberAtaques

Otros informes de talla internacional y generados por expertos en la política de ciberseguridad en Washington, como el informe "The Economic Impact of Cybercrime and Cyber Espionage", publicado por el Center for Strategic and International Studies (CSIS), informan sobre el crecimiento acelerado de piratas informáticos y que la gran mayoría de incidentes y delitos no vienen de un hacker externo sino que son cometidos por personas dentro de las mismas empresas, como por ejemplo empleados insatisfechos lo ocasionan grandes pérdidas no solo de información sino q se ven reflejadas en su disminución de ingresos.

IV. Guerra en Colombia

El conflicto armado en Colombia empieza alrededor de los años de 1960, los principales actores el Estado Colombiano: la guerrilla y los grupos paramilitares. Dicha guerra ha presentado fenómenos de violencia, el conflicto armado en Colombia se ha intensificado hasta dominar ampliamente el panorama general de la violencia en el territorio del país.

Ahora bien, se ve ese desplazamiento del conflicto bélico que toma el ciberespacio y las tecnologías a partir del año de 1999, como el "nuevo escenario de guerra". Durante los últimos años dichos ataques han aumentado notablemente y van desde una denegación de servicio (DoS), hasta ofensivas militares penetrando la seguridad de los sistemas informáticos atacando su infraestructura física, propagación de datos confidenciales a través de la red. Cabe aclarar, que a pesar de la existencia de la ley 1273/2009, aun quedan cabos por atar en el ámbito jurídico internacional ya que ese contexto no existe norma o regulación que tipifique los delitos de la guerra informática en el derecho internacional humanitario.

Aunado al conflicto interno, organizaciones como Anonymous, un grupo de hackers global que se especializa en protestar a través de la red y continuarán sus ataques cibernéticos a sitios de organismos oficiales por el impacto mediático que generan desequilibrio social. Tomando control de las páginas web de instituciones del estado como por ejemplo: Policía Nacional, de Presidencia, Ministerio del Interior y de Justicia, Ministerio de Defensa, el DAS, y del Partido de la U., Senado, como protesta por indignaciones a serias violaciones de los derechos humanos, estableciendo un ataque de denegación de servicio cerca de 18 horas, hackeando perfiles de twitter de reconocidas figuras política: Álvaro Uribe, Juan Manuel Santos.

No solo Colombia ha sido víctima de estos conflictos informáticos, la historia bien define guerras informáticas contra infraestructuras de países de todo el mundo: 1999 Guerra Kosovo penetrando computadores de la OTAN, 2003 Taiwán inactivando infraestructuras de hospitales y la Bolsa, 2006 Madrid interrupción de la línea del metro, 2007 Estonia afectando servicios de los medios de comunicación, bancos e instituciones gubernamentales, 2008 Georgia en contra de sitios del gobierno de dicho país, 2010 Irán uno de los escenarios más impactantes en la informática logrando atacar las centrifugadoras de la planta nuclear iraní el virus implantado fue llamado STUXNET y del cual fue acusado al gobierno de los Estados Unidos como autor principal, 2011 Canadá atacadas las páginas del ministerio de Finanzas, 2012 Medio Oriente atacado con un virus cuyo propósito es el ciber espionaje.

El despliegue de esas guerras bélicas a las informáticas afecta también notablemente las Fuerzas Militares de países que han buscado diferentes alternativas para combatir sus enemigos es así como Colombia adquirió hace aproximadamente cinco años seis equipos UAV, equipos no tripulados o sistemas aéreos no tripulados, también llamados drones. En un principio fueron comprados a Israel y más adelante resultado de la inversión de más de 2.000 millones de pesos, se han desarrollado prototipos Colombianos, construyendo aeronaves de 3,20 metros de envergadura capaces de participar en misiones de inteligencia y reconcomiendo operadas remotamente por personal de la Fuerza Aérea Colombiana como nueva estrategia para el combate militar. Esto demuestra más, que el futuro de la guerra interna del conflicto Colombiano toma un rumbo diferente al pensar en depender totalmente de la tecnología, no solo para operaciones de inteligencia y espionaje, sino también para inutilizar las defensas y plataformas del enemigo, lograr desestabilizar a un país o a un grupo armado al margen de la ley, causar pánico entre sus ciudadanos o llegar a pensar en tener la posibilidad de acceder a la información sensible o secreta a través de estrategias de ciberguerra son hoy en día la opción viable para poner fin a una guerra de mil años y son la solución a la que más apuntan los gobiernos incluyendo el Colombiano.

A la fecha grandes golpes del gobierno en contra de la guerrilla se han dado gracias a las buenas planeaciones de interceptaciones de llamadas, descifre de información y mensajes secretos; prueba fiel de ella fue la operación de ciberguerra llamada "Operación JAQUE" donde a través de medios tecnológicos fue posible crear tácticas de ataque e infiltrarse en las comunicaciones de la guerrilla gracias a la utilización de satélites Estadounidenses.

Es así, como se vislumbra en un futuro no muy lejano la degradación de los servicios informáticos en manos de delincuentes cibernéticos contratados por cualquiera de los frentes que intervienen en el conflicto de la guerra Colombiana con sus propios intereses y con un solo objetivo: "EL PODER".

V. Conclusiones

La precariedad de una normativa definida y bien tipificada para los delitos informáticos en Colombia se ha

convertido en la primera amenaza de una degeneración del estado Democrático de Colombia dejando expuestos a los usuarios de tecnologías sin demeritar los primeros esfuerzos plasmados en los artículos del código penal Colombiano.

Implementar nuevos hábitos, competencias y habilidades que permitan, de cierta forma, a los ciudadanos digitales contrarrestar los peligros y vacíos de exponer información personal en la Web, debería ser una de las grandes preocupaciones del gobierno Colombiano y en especial del ministerio de las Tics.

Los gobiernos están propensos a enfrentar una guerra por el dominio del ciberespacio sino toman la delantera en tecnologías de punta que ofrezcan una suite completa de herramientas de seguridad informática para blindar su información y las plataformas tecnológicas que manejan servicios indispensables para subsistir como el agua, la luz y las comunicaciones.

REFERENCIAS

[1] Ministerio de Defensa Nacional (2012). CiberSeguridad y Ciber Defensa: Una primera Aproximación: http://www.mindefensa.gov.co/irj/go/km/docs/MindefeMin/Documentos/descargas/estudios%20sectoriales/NotNo%20de%20Investigacion/Ciberseguridad%20y%20ciberdefen.pdf

[2] Diario El Espectador, 2012, Tecnología Ataques maliciosos se incrementaron un 81% en 2011.

[3] Eric Lair. Revista Colombia Internacional. (Número 49/50) Colombia: una guerra contra los civiles.

[4] María Gimena Rabinad Lecciones y Ensayos, nro. 85, 2008. La soberanía del ciberespacio, pág. 85-107.

[5] http://www.dinero.com/empresas_/articulo/colombia-segundo-pais-mas-sensible-ciberataques/159739

[6] Formato IEEE para presentar artículos http://ww.itsa.edu.co/ciit2010/Formato_Articulos_IEEEpdf