risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 20/09/2018
Aceitação/Acceptance: 21/11/2018

Modelo Ontológico de los Ciberdelitos: Caso de estudio Colombia

Jhon Marin[1], Yuri Nieto[2], Freddy Huertas[3], Carlos Montenegro[4]

Jhon.marin@cun.edu.co, yuri_nieto@cun.edu.co, fa.huertas@uniandes.edu.co, cemontenegrom@udistrital.edu.co

[1] Perito en Informática Forense Ciber GAULA Policía Nacional, Bogotá Colombia.

[2] Docente Corporación Unificada Nacional de Educación Superior CUN, Bogotá , Colombia

[3] Estudiante de Maestría de Ingeniería de Sistemas y Computación de Universidad de los Andes, Bogotá, Colombia

[4] Decano Facultad de Ingeniería Universidad Distrital Francisco José de Caldas, Bogotá, Colombia

Pages: 244–257

Resumen: Este articulo presenta un modelo Ontológico de los ciberdelitos tomando como caso de estudio Colombia. Se tienen en cuenta diferentes aspectos como son clasificación, jurisprudencia, nivel de impacto y se determinan las nuevas modalidades que se están presentando. A través del modelo ontológico se coleccionan conceptos clave y su interrelación colectiva con el fin de apoyar la toma decisiones en el ámbito de la ciberseguridad a través de la tipificación de los ciberdelitos. Este documento busca brindar herramientas que permitan reconocer el ciberdelito en Colombia, de igual forma, establecer patrones de conducta que permitan prevenir ser víctima de estos delitos y apoyar la toma decisiones respecto a la seguridad en la web.

Palabras-clave: Ciberdelitos; hackers; malware; ontología.

Ontological Model of Cybercrimes: Case study Colombia

Abstract: An Ontological model of cybercrimes is presented through the paper taking Colombia as a case study. Different aspects are taken into account such as classification, jurisprudence, level of impact and the new modalities that are currently in used. Through the ontological model, key concepts and their collective interrelation are collected in order to support decision-making on the cybersecurity field supported by typifying cybercrimes. This document seeks to provide tools that allow recognizing cybercrime in Colombia, in the same way, establish patterns of behavior that allow to prevent being a victim of these crimes and support decision-making in regard of web security.

Keywords*:* Cybercrimes; hackers; malware; Ontology.

1. Introducción

El Cibercrimen y su constante evolución, ha promovido que los delincuentes que anteriormente actuaban de manera aislada, sin coordinación, con un alcance local y corriendo riesgos al realizar sus actividades de forma presencial, se constituyan en empresas criminales, con roles específicos dentro de una organización, adicionalmente cuentan con recursos económicos y de software, así como alcances ilimitados y total anonimato.

El mercado ilegal de datos y el ciber crimen como servicio han facilitado su auge y transformación, así como, el fácil acceso al mercado ilegal de Malware (programas maliciosos), las monedas virtuales y la dificultad de rastreo de actividades ilícitas en la internet profunda o Dark Net.

Aunque desde 1983 comenzó a hablarse de la criminalidad informática y en 1992 se acuñó el término Cibercrimen (Fernando Miró Llinares. 2012), el fenómeno de la criminalidad relacionada con el uso de las Tecnologías de la Información y la Comunicación sigue siendo novedoso y por ello, parcialmente incomprendido por la sociedad en general y en particular, por las instituciones encargadas de la prevención de esta amenaza.

Según Microsoft, Colombia es el tercer país en Latinoamérica con mayor índice de Cibercrimen. De acuerdo con cifras avaladas por el IDC Colombia (empresa dedicada al análisis del mercado de Tecnología Informática y Telecomunicaciones), los ciberataques han aumentado entre el 30% y el 40% en América Latina, una de las zonas con mayor actividad en el mundo. Durante 2015, se registraron más de 20 violaciones a la seguridad por segundo en la región, lo cual equivale a 400 mil vulneraciones a causa de virus. Por su parte, en el mismo año, Colombia ha sido el tercer país más afectado por el Cibercrimen con 5 millones de ataques informáticos, seguido de Brasil y México con 27 millones y 16 millones de incidentes de este tipo respectivamente **(**http://www.microsoftcolombia.com/dia-de-cibercrimen-colombia**).**

La ontología es una base importante para el conocimiento que representa el mundo real (Yang 2009). La filosofía acuño el término de ontología y ha ido creciendo en el campo de la informática y el sistema de información (Koutero, Fujita y Sugawara 2010) (Maedche y Staab 2002) (Busagala et al., 2008). Hoy en día, el término ontología se usa en numerosos campos de Ingeniería, la ontología que se presenta en el artículo busca de forma clara, clasificar los ciberdelitos según su tipo de ataque y objetivo, definiendo su jurisprudencia en Colombia, su impacto y las nuevas modalidades que se presentan. Brindar a la sociedad un conocimiento claro de las malas conductas en la web y como estas son tipificadas y reconocidas por el gobierno como un delito, les brindará así mismo el apoyo necesario para tomar decisiones referentes a su seguridad en la web.

El presente artículo tiene como objetivo definir un modelo Ontológico del ciberdelito tomando como caso de estudio a Colombia. En la segunda sección se define el modelo ontológico del Cibercrimen tomando como caso de estudio Colombia. Se muestra en la tercera sección la definición del ciber crimen. En la cuarta sección ciber guerra y ciber defensa, por último, en la quinta sección se presentan las conclusiones y trabajo a futuro.

2. Definición ontológica del ciber crimen

En la figura 1 se plantea el Modelo Ontológico del Ciber crimen, definiendo los tipos de ataques que se pueden realizar y su tipicidad en el código Penal.

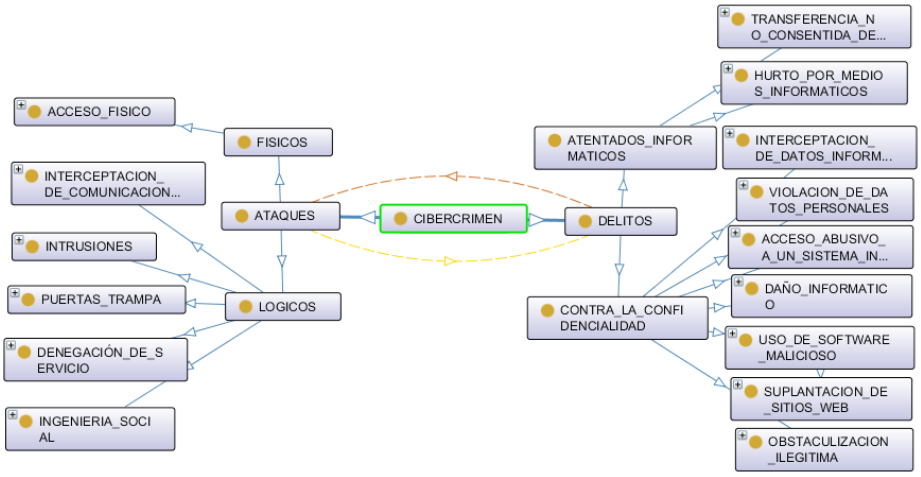

Figura 1 – Modelo Ontológico del ciber crimen

Para llevar a cabo la definición ontológica, se tomó como referente las leyes colombianas y en específico el código penal colombiano. El Cibercrimen se divide en ciberataques. Estos son la forma como se realiza la conducta y en cómo se tipifican estas conductas en el código penal colombiano.

2.1. Ciber ataques

Los sistemas informáticos están compuestos por cierta cantidad de componentes que permiten su correcto funcionamiento, entre ellos, electricidad, hardware, sistema operativo, aplicaciones, datos, red, usuarios, entre otros. Los ataques se pueden realizar en cada eslabón de esta cadena, aprovechando las vulnerabilidades que el atacante explote, es así, que se pueden presentar los siguientes ataques:

2.1.1. Acceso físico

El atacante tiene acceso a las instalaciones e incluso a los equipos:

- Interrupción del suministro eléctrico, su objetivo es generar daño físico a los equipos, causando fallas en el sistema eléctrico.
- Apagado manual del equipo, se realiza de forma presencial y busca la perdida de información.

- Vandalismo, a través de ataques físico causar daños a la infraestructura.
- Apertura de la carcasa del equipo y robo del disco duro.
- Monitoreo del tráfico de red, con el fin de detectar vulnerabilidades que puedan ser explotadas en futuros ataques.

2.1.2. Interceptación de comunicaciones

El atacante busca recopilar la información de acceso y de esta forma tener acceso restringido al sistema.

- Secuestro de sesión, robo de perfiles o de identidad del usuario.
- Falsificación de identidad, a través de phishing, simular la identidad de un usuario o de una página.
- Re direccionamiento o alteración de mensajes, se usa para realizar ataques tipo troyano, simulando ser un correo de confianza.

2.1.3. Denegaciones de servicio

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Su objetivo es interrumpir el funcionamiento normal de un servicio.

- Explotación de las debilidades del protocolo TCP/IP.
- Explotación de las vulnerabilidades del software del servidor.

2.1.4. Intrusiones

Es un ataque el cual busca dar acceso a personal no autorizado a un sistema informático, otorgándole privilegios de administrador o incluso acceder a información reservada.

- Análisis de puertos, Una técnica que los hackers usan para encontrar las debilidades de un equipo o de una red. Si bien esta técnica no es un ataque en realidad, los hackers la usan para detectar qué puertos están abiertos en un equipo. De acuerdo con la información de los puertos abiertos, puede obtenerse acceso no autorizado.
- Elevación de privilegios: este tipo de ataque consiste en aprovechar una vulnerabilidad en una aplicación al enviar una solicitud específica (no planeada por su diseñador). En ciertos casos, esto genera comportamientos atípicos que permiten acceder al sistema con derechos de aplicación. Los ataques de desbordamiento de la memoria intermedia (búfer) usan este principio.
- Ataques malintencionados (virus, gusanos, troyanos).

2.1.5. Ingeniería Social

En la mayoría de los casos, el eslabón más débil es el mismo usuario. Muchas veces es él quien, por ignorancia o a causa de un engaño, genera una vulnerabilidad en el sistema al brindar información (la contraseña, por ejemplo) al pirata informático o al abrir un archivo adjunto.

2.1.6. Puertas trampa

Son puertas traseras ocultas en un programa de software que brindan acceso a su diseñador en todo momento.

Es por ello que los errores de programación de los programas son corregidos con bastante rapidez por su diseñador apenas se publica la vulnerabilidad.

2.2. Delitos informáticos

En Colombia se tipificaron en el Código Penal los delitos informáticos, los cuales se dividen en: delitos contra la confidencialidad y atentados informáticos.

2.2.1. Delitos contra la confidencialidad

Son aquellos atentados contra la confidencialidad personal, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

- Acceso abusivo a un sistema informático: se refiere al que sin autorización, acceda a un sistema informático protegido en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.
- Obstaculización ilegítima de sistema informático o red de telecomunicación: incurre en esta conducta el que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos o a una red de telecomunicaciones.
- Interceptación de datos informáticos: se refiere al que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático.
- Daño Informático: lo realiza quien, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.
- Uso de software malicioso: se refiere al que, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.
- Violación de datos personales: lo realiza quien con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.
- Suplantación de sitios web para capturar datos personales: se refiere a la persona que con objeto ilícito diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

2.2.2. Atentados informáticos

Son aquellos ataques que no transgreden la información personal, pero que producen un daño o un detrimento económico a través del entorno digital.

- Hurto por medios informáticos y semejantes: hace referencia al que, superando medidas de seguridad informáticas, hurte manipulando un sistema informático,

una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

- Transferencia no consentida de activos: la comete la persona que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero.

3. Ciber crimen

Pocos años atrás, los programas maliciosos se limitaban al "ciber-vandalismo", una forma de expresión antisocial que irrumpía en los PCs causando diversos daños. Pocos de ellos, no obstante, estaban diseñados con este fin, e inevitablemente producían daños colaterales en los archivos o dejaban el equipo inservible. La mayoría de las amenazas en esta época consistían en virus y gusanos.

Hoy en día, por el contrario, la amenaza más grave proviene del llamado Cibercrimen. (Miro 2015) Los criminales se sirven del anonimato que la red otorga para, mediante códigos maliciosos, acceder a los equipos y robar dinero o datos confidenciales como contraseñas, logins, códigos PIN, etc.

Las amenazas del Cibercrimen incluyen: virus, gusanos, troyanos, ataques de hackers, phishing demás. Estas amenazas son cada día más sofisticadas y su número crece exponencialmente.

Cuando se hace referencia a cibercrimen se entiende que se trata de delitos cometidos a través de internet por medio del uso de un computador o mecanismo análogo (por ejemplo: smartphone, pendrive, tablet, etc.). También se han empleado términos tales como computer crime, computer related crime, digital/electronic/virtual, IT, high tech-crime, delitos informáticos, entre otros (Miró 2011).

Todos los usuarios de la web, de manera directa o indirecta están expuestos a ser víctimas de fraude, extorsión y espionaje informático. Este delito, mejor conocido como Cibercrimen, no sólo pretende conseguir un beneficio principalmente económico, sino que también abarca el dominio de Internet como ataques con fines políticos, programas informáticos maliciosos, etc.

Cuando se hace referencia a cibercrimen se entiende que se trata de delitos cometidos a través de internet por medio del uso de un computador o mecanismo análogo (por ejemplo: smartphone, pendrive, tablet, etc.). También se han empleado términos tales como computer crime, computer related crime, digital/electronic/virtual, IT, high tech-crime, delitos informáticos, entre otros.

3.1. Ciber crimen en Colombia

Según el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC) 8 de cada 10 colombianos usan actualmente internet, el Ministerio TIC e Ipsos Napoleón Franco presentaron el estudio de Consumo Digital, donde se revela cómo, dónde, cuándo y cada cuánto los colombianos usan Internet (http://www.mintic.gov.co/portal/604/w3-article-1629.html, s.f.).

El estudio reveló que el 80% de los encuestados usa Internet y que el mayor incremento del uso de la red se dio en los estratos 1 y 2, con un crecimiento del 17% en comparación al uso que le daban en 2010. También se observa que el 54% de los colombianos que usan Internet, lo hacen todos los días y pasan en promedio 2,6 horas navegando.

Si bien es cierto que Colombia es pionera en América Latina en temas de conectividad y acceso a internet, esto ha provocado que más personas sean propensas a ser víctimas del ciber crimen, debido a que aunque se logró mayor conectividad y mayor acceso a las nuevas tecnologías; no se realizó el mismo esfuerzo para capacitar a los ciudadanos sobre el uso adecuado de internet.

3.1.1. Estrategias del gobierno colombiano

El 14 de julio de 2011, se realizó en Colombia el CONPES 3701 (Consejo Nacional de Política Económica y Social) LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA, el cual buscaba generar lineamientos de política en Ciberseguridad y Ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

La problemática central se fundamentó en que la capacidad actual del Estado para enfrentar las amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. Para la aplicabilidad de la estrategia se definen recomendaciones específicas a desarrollar por entidades involucradas directa e indirectamente en esta materia. Así lo ha entendido el Gobierno Nacional al incluir este tema en el Plan Nacional de Desarrollo 2010-2014 "Prosperidad para Todos", como parte del Plan Vive Digital.

Dicho CONPES se realizó teniendo en cuenta los ciberataques perpetuados en varias partes del mundo y los ocurridos en Colombia, debido a esto se creó la Ley 1273 de 2009, con la cual se creó un nuevo bien jurídico tutelado "de la protección de la información y de los datos".

El gobierno Colombiano no podía ser indiferente ante los cambios que se estaban presentando en el mundo, donde aparecieron grupos hacktivistas como anonimous que demostraron tener la capacidad de burlar y bloquear cualquier sistema. Es por ello que, al no existir legislación vigente para investigar estos delitos, se creó esta Ley mediante la cual se tipificaron los ciberdelitos en el código penal colombiano.

3.1.2. Impacto del ciber crimen en Colombia

Según la compañía de ciber seguridad Digiware, Colombia participó con el 8,05% del total de los delitos informáticos de América Latina, lo que equivale a pérdidas por más de US$6.179 millones. Con estas cifras, Colombia es quinto en la clasificación latinoamericana en materia de ataques informáticos.

Digiware mostró que Brasil es primero y representa el 25,13% de los ataques a nivel regional, seguido por México con 15,53%, Venezuela 11,91% y Argentina con 9,63%.

Diariamente, en Colombia se producen en promedio 542.465 ataques informáticos. Así se distribuyen los ataques por sectores económicos (sectores-mas-afectados-por-cibercrimen-en-colombia/250321):

El sector financiero: 214.600 ataques por día (39,56%).

Telecomunicaciones: 138.329 ataques por día (25,5%).

El sector Gobierno: 83.756 ataques por día (15,44%)

Sector energético: 19.583 ataques por día (3,61%)

Industria: 51.263 ataques por día (9,45%).

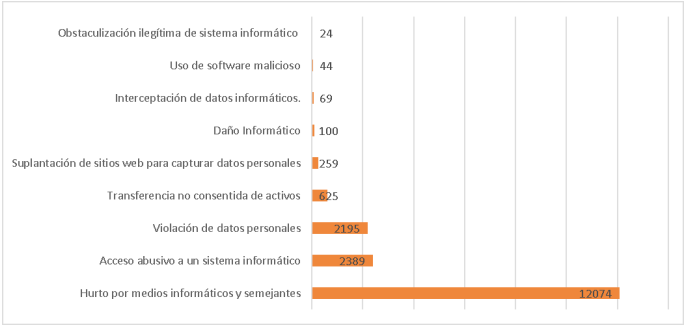

Figura 2 – Denuncias de delitos informáticos en Colombia

En la figura 2 se observa que entre el año 2014 y 2017, se recibieron 17.779 denuncias por violación a la ley 1273 de 2009, dando un panorama de los delitos que más se denuncian en el país. En cuanto a las tipologías criminales denunciadas ante la Policía Nacional en

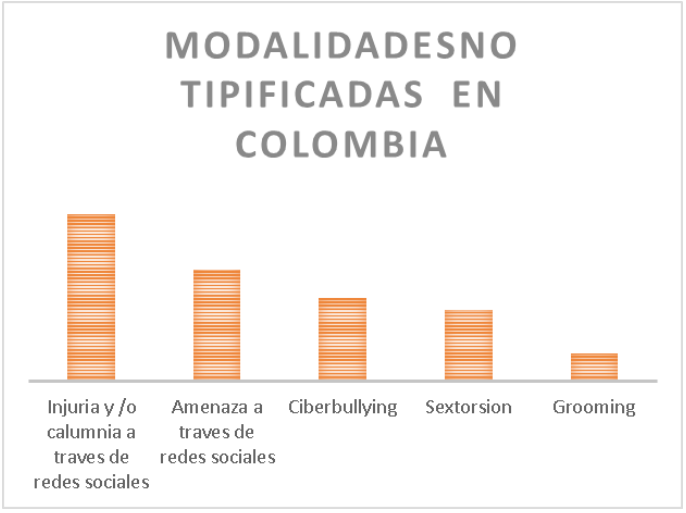

Figura 3 – Modalidades no tipificadas en Colombia

el citado periodo de tiempo, se evidencia un aumento significativo en el número de estas por conductas delictivas que vulneraron la integridad personal, patrimonio económico de entidades público - privadas, así como la integridad, disponibilidad y confidencialidad de la información que circula a través del ciberespacio.

El hurto por medios informáticos y semejantes es la tipología criminal de mayor frecuencia, equivalente al 68%, seguido del acceso abusivo a un sistema informático con el 13% y violación de datos personales con 12% de la muestra.

Se refleja con esto, que las intenciones cibercriminales desde y hacia Colombia están ligadas principalmente a los campos comerciales y financieros, afectando tres aspectos primordiales que soportan el comercio electrónico que son: confianza, sistemas de pago y seguridad.

En la figura 3, se puede observar las modalidades más frecuentes de los ciberdelitos en Colombia. Este tipo de modalidades afectan en su gran mayoría a los niños, niñas y adolescentes con un 75%, teniendo en cuenta que son más susceptibles al engaño y vulnerables en el ciberespacio.

Figura 4 – Mapa de calor ciber ataques en Colombia

En la figura 4, se evidencia que la mayor cantidad de ataques en Colombia se presentan en las ciudades capitales, las principales ciudades con más reportes de incidentes informáticos se observan en la tabla 1.

4. Ciber Guerra y Ciber Defensa

El término de ciberguerra se refiere a aquella lucha desarrollada en el espacio virtual, en donde actores estatales y no estatales se enfrentan por beneficios particulares e incluso altruistas, dejando de paso pérdida de información, propiedad intelectual y hasta económica.

La ciberguerra en un nivel profundo se trata de conocimiento, acerca de quién sabe, cuándo, dónde, qué, y por qué, así como cuán segura es una sociedad o estamento militar con respecto al conocimiento de sí mismo y de su adversario (Riascos 2015).

REPORTE DE INCIDENTES INFORMATICOS	
CIUDAD	CANTIDAD
BOGOTA	9709
MEDELLIN	691
CALI	475
BARRANQUILLA	240
BUCARAMANGA	1273
CIUDADES CON MAS DENUNCIAS LEY 1273	
BOGOTA	2607
CALI	1607
MEDELLIN	998
BUCARAMANGA	594
IBAGUE	448
BARRANQUILLA	398

Tabla 1 – Reporte de incidentes y denuncias en Colombia.

Similarmente el concepto de ciberpoder, al cual se refiere como un "conjunto de recursos relacionados con la creación, control y comunicación de información basada en sistemas electrónicos y computacionales, esto incluye no solo la internet, computadores conectados en red, sino también intranets, tecnología celular y comunicaciones satelitales" (universidad externado de colombia 2017).

Ciberguerra y ciberpoder guardan una relación absoluta, la cual está orientada al control de un recurso clave que alimenta el poder de un actor sobre otro, esto es, la información como elemento decisivo en el ciberespacio o en un campo de batalla real (Vasquez 2015).

Es evidente que el Cibercrimen y los fenómenos acordes que se ciernen en un espacio virtual que carece de soberanías, representan sobre el mundo tangible, caracterizado por territorialidades e intereses, una amenaza de difícil control por parte de un Estado, sin alianzas estratégicas y grupos colaborativos tanto a nivel nacional como internacional.

En este sentido, las consecuencias en términos distributivos dada la interdependencia económica en el sistema internacional y la existencia de jurisdicciones nacionales, crean un interés e incentivo común que, según Keohane (1984), es el principio para el desarrollo de la cooperación entre Estados. En un sentido similar, la dificultad de persecución sobre actores atomizados y dispersos en el mundo hace necesaria la cooperación policiva entre agencias de seguridad nacionales y transnacionales, a la hora de perseguir en el mundo físico crímenes y acciones que hallan su base de operación en un mundo informático.

Las Fuerzas Armadas alrededor del mundo se preparan desde hace tiempo para las batallas y guerras en un nuevo escenario cyber. Toda actividad bélica en nuestros días trae consigo más allá de los medios y métodos tradicionales, una estrategia de ciberataques para debilitar, confundir o suprimir al enemigo. Las guerras en el siglo XXI tienen un mayor componente digital y de la información que nunca. También las técnicas de la guerra experimentan transformación digital.

Cabe recordar que la segunda confrontación global fue una victoria para los Aliados en gran medida por las Tecnologías de la Información, con el Profesor Alain Turing y los sabios -precursores de los científicos informáticos- que lo acompañaban descifrando las ordenes y mensajes de los comandantes Nazis. (Nye 2011) Luego con el uso de la tecnología nuclear por los EEUU en Hiroshima y Nagasaki se ratificó que estábamos como género humano cada vez más lejos de la confrontación física y las TIC a gran escala se tomaban el escenario de la guerra.

Hoy en día la profundización de esa tendencia con la combinación de tecnologías como robótica, drones, inteligencia artificial y big data para las nuevas confrontaciones. Los sistemas de información públicos y privados y las infraestructuras esenciales son el blanco de las nuevas tecnologías de la guerra. La ciberdefensa exige un blindaje, barreras de entrada, políticas, prácticas, estrategias para evitar las consecuencias de ataques devastadores.

4.1. Ciber ataque y Ciber defensa

La estrategia ciberbélica busca generar poderosas armas que permitan de ser necesario una ofensiva y agredir a los enemigos causando los mayores daños y mayores beneficios. También se requiere la defensa adecuada de los bienes digitales y de los sistemas de información. Las barreras y escudos que blinden a recursos críticos e instalaciones esenciales.

Las armas ofensivas y las defensivas deben ser disuasivas para que los países enemigos o con intereses opuestos no se atrevan a atacar. Los nuevos arsenales de los países están enfocados en el ciberespacio. La vigilancia, el robo de información o la destrucción son los principales objetivos de las cyberweapons.

En el reciente ataque internacional Wanna Cry, el arma desarrollada por una agencia de inteligencia aparentemente de EEUU y el escenario global de muchos equipos

Figura 5 – Ciber ataques en el mundo (http://www.norse-corp.com/)

informáticos con vulnerabilidades en Código no actualizado, conectados ampliamente a internet y a redes internas.

La guerra digital utiliza medios a distancia, no presenciales. Las armas no tienen control mediante tratados internacionales como sí ocurre por ejemplo con la proliferación de armas nucleares.

La ética del soldado, el límite del ser humano en la confrontación con el otro ahora encuentra un esguince, la inteligencia artificial como arma bélica.

Cada país en ejercicio de soberanía y con la mira en el cumplimiento del deber general de defensa de la vida, honra y bienes debe llevar a cabo una transformación digital de sus estrategias, tácticas, medios de defensa y ataque en el ecosistema digital.

Como se observa en la figura 5, los ciber ataques en el mundo se dan a cada segundo y son cada vez más frecuentes entre potencias mundiales, que al parecer, ya se encuentran en una guerra no declarada a través del ciber espacio.

4.2. Política de ciberdefensa en Colombia

En Colombia, la política pública que concierne a los temas de seguridad digital se estableció inicialmente en el documento CONPES 3701 de 2011, que incluye los lineamientos de política para ciberseguridad y ciberdefensa. Esta política busca mitigar los riesgos derivados de las amenazas informáticas y desarrollar políticas de prevención y control. La Política crea el sistema de seguridad digital coordinado por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), junto con el Centro Cibernético Policial (CCP) y el Comando Conjunto Cibernético (CCOC). EL ColCERT coordina los Equipos de Respuesta ante Incidencias de Seguridad (CSIRT). Las funciones compartidas por estas instituciones están encaminadas a: 1) responder a los incidentes informáticos, 2) responder a la amenaza de los delitos informáticos y 3) velar por la seguridad digital nacional.

En 2016, mediante el documento Conpes 3854 se determinó una nueva política de seguridad digital. El documento parte de una visión más enfocada a restablecer la confianza de los usuarios y lograr que el ecosistema digital sea una plataforma segura para los negocios electrónicos también desarrolla el principio de la responsabilidad compartida entre las múltiples partes interesadas en el cual cada sujeto tiene un grado de responsabilidad en la gestión de los riesgos de seguridad y en proteger el entorno digital. La nueva visión comprende la gobernabilidad participativa de múltiples partes interesadas, y definir los niveles de escalamiento para el reporte de incidentes digitales.

En Colombia se han creado laboratorios de ciber, quienes se encargan de combatir el ciber crimen, recolectar evidencia digital y analizarla, perseguir ciberdelincuentes a través de la red, lo cual no es tarea fácil, más aun cuando un ataque se puede realizar desde cualquier computadora conectada a la red

Los talentos en desarrollos digitales, en las novísimas tecnologías deben hacer parte de las nuevas Fuerzas Armadas, consolidar nuevos “batallones cyber” y consolidar estrategias de defensa.

A escala global crece la discusión sobre la aplicación de las reglas tradicionales sobre el derecho de la guerra entre las naciones, Convenios de Ginebra de 1949 y Protocolos Internacionales pueden aplicarse al nuevo escenario de la guerra digital.

En suma, a la tierra, mar y aire como elementos distintivos de las distintas Fuerzas Armadas se debe incorporar el ciberespacio. Otro reto para varias generaciones en el Siglo XXI.

5. Conclusiones y Trabajo Futuro

Al realizar el modelo ontológico de los ciberdelitos tomando como caso de estudio Colombia, se logró definir que los ciberdelitos están compuestos por la forma en que se realiza el ataque y su definición punitiva en el código penal, permitiendo establecer la relación entre la forma en que se realiza la conducta y su tipicidad.

Se tienen en cuenta diferentes aspectos como son clasificación, jurisprudencia, nivel de impacto y se determinan las nuevas modalidades que se están presentando. A través del modelo ontológico se coleccionan conceptos clave y su interrelación colectiva con el fin de proporcionar una vista abstracta y tipificar así mismo los ciberdelitos. Una ontología es una colección de conceptos clave y su interrelación colectiva con el fin de proporcionar una vista abstracta de cualquier dominio de aplicación, con el fin de tipificar acertadamente los ciberdelitos. Este documento busca brindar herramientas que permitan reconocer el ciberdelito en Colombia, de igual forma, establecer patrones de conducta que permitan prevenir ser víctima de estos delitos.

El cambio social ha determinado el surgimiento de nuevos riesgos que se materializan en nuevas fenomenologías criminales. Los cibercrímenes representan, justamente, el nacimiento de comportamientos que, en su sentido puro, como delitos informáticos en sentido estricto, tienen lugar en realidades virtuales o simuladas como el ciberespacio, protegen objetos inmateriales como los datos y la información y tutelan nuevos bienes jurídicos intermedios. Si a ello se suma el hecho de que estos delitos son realizados mediante técnicas particulares (que en muchos casos consisten en la manipulación de energía o bytes basados en sistemas binarios, que pueden ser traducidos a los humanos mediante infraestructuras informáticas o Hardware), se aprecian delitos que distan mucho de ser asimilables a los delitos tradicionales.

Parece necesario y relevante complementar las categorías tradicionales del delito en la tipicidad, con una perspectiva digital que, por cierto, ya no es la excepción a la regla, sino que comienza a ser la regla general en la criminalidad moderna. Esto incluso en ámbitos hasta ahora reservados a la criminalidad física, como la criminalidad organizada y transnacional, que comienza a actuar mediante organizaciones virtuales transnacionales (OVT) que dificultan aún más combatir este tipo de delincuencia sin fronteras.

En Colombia por ser un país con un alto índice de conectividad a internet, está expuesto a los diferentes tipos de ciber ataques, sumado a esto, el nivel de capacitación acerca de la navegación segura y la prevención hacia los delitos informáticos es muy baja, siendo así que muchos colombianos navegan, pero pocos saben hacerlo de manera responsable y segura. De igual forma, la denuncia de estos delitos es muy baja, ya que las personas ignoran que muchas de las conductas de las cuales son víctimas, se consideran un delito y están tipificadas en el Código Penal, lo cual dificulta que se ataque el fenómeno delictivo de forma certera y efectiva.

A futuro se investigará sobre como nuevas tendencias del ciber crimen en el mundo impactan a Colombia.

Referencias

Ontological Knowledge Model to Engineering Project Integration Based on PMS. MSc(c). Yuri Nieto 1, Dr. Roberto Ferro 2, Dr. Carlos Montenegro3

El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. Fernando Miró Llinares. 2012 http://www.microsoftcolombia.com/dia-de-cibercrimen-colombia.

Design of an Assisting Agent Using a Dynamic Ontology, Alexis Koutero, Shigeru Fujita, Kenji Sugawara, 2010

Yang, D.: Product Configuration Knowledge Modeling Using Ontology Web Language. Expert Systems With Applications 36(3), 4399–4411 (2009)

L. S. P. Busagala, W. Ohyama, T. Wakabayashi, and F. Kimura, "Improving automatic text classification by integrated feature analysis," IEICE Trans. Inf. Syst., vol. E91-D, no. 4, pp. 1101–1109, Nov. 2008.

Y. Sure, J. Angele, and S. Staab, "OntoEdit: Guiding ontology development by methodology and inferencing," Lect. Notes Comput. Sci., vol. 2519, pp. 1205–1222, 2002. (http://www.mintic.gov.co/portal/604/w3-article-1629.html, s.f.) (http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf, s.f.)https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321 https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real

Arquilla y Ronfeldt (1993, p. 27) Nye (2011, p. 123)

Nada volverá a ser igual: ciberguerra y ciberpoder. Autor Javier Alberto Castrillón-Riascos, 2015.

Nos llegó la Ciberguerra. Universidad externado de Colombia. 2017

Propuesta de buenas prácticas para fortalecer los controles de prevención y detección temprana del cibercrimen en las empresas colombianas. Autores Vásquez Zarate, Katy Alejandra Cárdenas Rodríguez, María Paula, 2015.

Ciber crimen y vida diaria en el mundo 2.0, Dr. Fernando Miro Linares, 2015.

Miró, La oportunidad criminal en el ciber espacio, revista electrónica de ciencia penal y criminología, 2011. http://www.norse-corp.com/

Miró, el ciber crimen, fenomenología y criminología de la delincuencia en el ciber espacio, 2012.

Miro, La oportunidad criminal en el ciber espacio, 2011.