CAPÍTULO III

# EL IMPACTO DE LA ACADEMIA EN LA CIBERSEGURIDAD*

*Alejandro Bohórquez-Keeney*

Capítulo de libro resultado del proyecto de investigación titulado "Gestión de Riesgos en seguridad Digital" de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, que a su vez hace parte de la línea de investigación "Seguridad Digital" del grupo de investigación "Masa Crítica", reconocido y categorizado en (B) por Colciencias. Registrado con el código COL0123247, está adscrito a la Escuela Superior de Guerra "General Rafael Reyes Prieto" de la República de Colombia.

## Introducción: academia y seguridad

La aparición del ciberespacio ha alterado todos los espacios de la vida cotidiana, llevando así a transformaciones importantes en las instituciones sociales, políticas y de seguridad; llegándosele a considerar hoy en día como el quinto campo estratégico. Precisamente, esta particularidad del ciberespacio de permear todos los sectores sociales hace que ninguna institución pueda abstraerse de este, en particular de las amenazas que provienen del campo estratégico artificial. De ahí, la importancia de que el sector académico haga presencia en los programas y las políticas públicas que aborden la ciberseguridad.

De entrada, la educación es considerada como servicio esencial para el mantenimiento de las funciones sociales básicas del Estado, y por ello hace parte de la infraestructura informática crítica de Colombia (CCOC, 2015). Al recordar que parte de lo que constituye la Infraestructura Informática Crítica es un nivel material donde se encuentran los servidores, conexiones, satélites y aparatos que son utilizados para acceder al ciberespacio, a la vez de un nivel inmaterial que corresponde a la información almacenada y distribuida por dicha infraestructura (Dunn & Suter, 2012). Por tales motivos, el sector académico es clave teniendo en cuenta que dentro de las universidades se encuentra un importante componente de la infraestructura física del ciberespacio, como también la importancia de la información que se maneja en las instituciones académicas. Adicionalmente, por su función social es al sector académico al que le correspondería la capacitación y entrenamiento en cuestiones de ciberseguridad.

En el presente capítulo, se examinará el estado de la cuestión pertinente al papel desempeñado por la academia dentro de la seguridad digital. En primer lugar, se revisarán las principales políticas públicas en materia de ciberseguridad dentro de la región, al igual que de otros países de interés; haciendo un énfasis particular en el papel que desempeña el sector Educación dentro de ellas. Esto con el fin de entender cómo han sido las concepciones que se tiene de este sector como parte fundamental de la Infraestructura Informática Crítica. En principio, se tomarán en cuenta los actores regionales que por su relevancia vale la pena considerar, para luego mirar casos de interés en el hemisferio norte.

En segundo lugar, se revisarán los documentos académicos que hagan mención directa, o que se aproximen de manera suficiente, a los acercamientos que ha hecho la academia en su papel definido dentro de la Infraestructura Informática Crítica. Para poder lograr este perfilamiento del sector académico, se tomarán en cuenta los resultados que arroje la revisión hecha en el aparte anterior, sumado al resultado de las mesas de trabajo realizadas por la Maestría de Ciberseguridad y Ciberdefensa frente al tema de la gestión de riesgos en seguridad digital. El eje central de esta segunda revisión es la ejecución de las políticas públicas en seguridad digital, y cómo se han llevado a cabo hasta el momento, de ahí, la necesidad de perfilar primero el rol de la academia en este campo.

En tercer lugar, se hará una nueva revisión documental, pero en este caso se basará en la proyección a futuro que se hace del sector académico en el ámbito de la ciberseguridad. De este modo, se busca visibilizar las posibles fortalezas que se esperan desarrollar, así como los futuros retos que pueden aparecer, entendiendo que la complejidad del ciberespacio hace que este sea un entorno altamente variable. Así las cosas, puede hacerse un balance más definido y detallado de la importancia del sector académico como actor primordial de la ciberseguridad de un Estado, y en particular, Colombia.

Finalmente, se presentarán unas conclusiones donde se relacionan todos los hallazgos encontrados en esta investigación, y aportar de esta manera, posibles escenarios y recomendaciones frente al tema propuesto. Por ende, este capítulo busca ir más allá de una mera recopilación

documental, y ser propositivo para nuevas investigaciones y proyectos relacionados con la seguridad Digital, y más con la academia como actor principal.

## 1. Políticas públicas, academia y seguridad digital

Como se mencionó en la introducción, en este aparte se hará una revisión de las políticas públicas en ciberseguridad, y cuál es el papel y las funciones que estas le otorgan al sector académico a desempeñar en este campo. Por un lado, se tomarán en consideración las políticas de los principales actores de la región, debido a que su proximidad con Colombia los hace principales socios estratégicos en caso de lograrse tratados regionales sobre seguridad digital, además de las posibles lecciones a aprender de ellos. Por otro lado, se revisarán las políticas elaboradas por los países líderes en el tema de ciberseguridad, cuyo acceso sea abierto a la revisión por parte de personal externo a sus entidades estatales.

Antes de continuar, vale aclarar que de acuerdo con el Banco Interamericano de Desarrollo (BID), existe una falta de conciencia en la región sobre la ciberseguridad, a causa de una ausencia por parte del sector académico en este tema. Puntualmente, "pocos países ofrecen programas de educación a nivel posgrado para la seguridad cibernética, y los programas de formación profesional son más comunes, pero varían en calidad" (Foro Económico Mundial, 2016, p. 26). Esto, ya denota los grandes vacíos y retos que afronta el sector académico, no solo en Colombia, sino también en la región, al no apropiarse de un tema que como se mencionó le es vital. A causa de esto, para conocer cómo el tema de la ciberseguridad afecta la academia, es que se toma esta revisión de políticas públicas.

Inicialmente, aquí en Colombia el *CONPES 3854 de 2016* enfatiza el sector Educación como parte de la Infraestructura Informática Crítica, y como una de las múltiples partes interesadas que dependen del entorno digital para su buen funcionamiento. De hecho, de acuerdo con este documento la educación y el aprendizaje ocupan un 36.7 % de la actividad

ciberespacial nacional (CONPES 3854 de 2016), lo que resalta la importancia de este sector dentro del entorno digital colombiano. Aun así, el papel que se le asigna a este sector se limita a la capacitación y difusión de buenas prácticas, sin que se le determinen acciones más proactivas en materia de ciberseguridad.

Igualmente, Chile en su Política Nacional de seguridad advierte la necesidad de la participación activa de su respectivo sector académico, pone como labor principal de este, la formación en buenas prácticas cibernéticas. De manera similar al *CONPES 3854 (2016)*, la política chilena de ciberseguridad aborda este reto desde todos los niveles educativos, subrayando la necesidad de la instrucción de dichas prácticas desde una edad temprana. De esta forma, son claros y particulares a los retos y desafíos a los que se enfrenta el sector académico del país austral.

De manera análoga y muy similar, México (2017) en su Estrategia Nacional de ciberseguridad ubica también al sector académico como jugador clave y capacitador en materia de su propia seguridad informática. Esta estrategia, es bastante insistente en la idea de establecer acciones coordinadas entre el sector académico y demás partes interesadas (México, 2017), aunque no establece planes de acción claros y su contenido sigue siendo muy general. En este instante, ya se puede ir adelantando una conclusión respecto a la participación del sector académico en la ciberseguridad, y es que su papel se define más desde la participación que desde la acción.

Por su parte, Brasil presenta un caso interesante para las políticas de ciberseguridad, al no contar con una sino con tres de ellas en su proyección de liderazgo regional, siendo estas: la *Política Cibernética de Defesa* y la *Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal* (2015-2018) (Cruz Lobato, 2017). La primera de ellas, se concentra exclusivamente en Ciberdefensa, y por este motivo es de alcance exclusivamente militar (Estado-Maior Conjunto das Forças Armadas, 2014); en cambio la segunda, la academia, es identificada como sector estratégico de la ciberseguridad, y se establece como prioridad su cooperación y creación de redes de información con este (Departamento de Segurança da Informação e Comuni-

cações, 2015). A diferencia de las políticas referenciadas anteriormente, no hace explícita la necesidad de que el sector académico se encargue de la capacitación y formación de expertos en ciberseguridad, o de buenas prácticas digitales.

En el caso peruano, se trata de una política de ciberseguridad muy incipiente que apenas contempla al sector académico como parte interesada en este campo, mas no presenta un curso de acción específico (Secretaría de Gobierno Digital, 2017). Ni qué decir, de lo que sucede en Argentina, donde existe una normatividad sobre seguridad, pero no una política pública como tal (Gobierno de Argentina, 2018), y a pesar de contar con el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), a la fecha que esto se escribe, aún está en sus planes desarrollar una política pública en ciberseguridad (ICIC, 2018). Así entonces, se revela que el desarrollo en ciberseguridad dentro de la región es aún muy precario, y de ahí parte la dificultad de rastrear programas específicos para el sector académico en este campo.

Ahora bien, llevando la mirada al hemisferio norte se pueden encontrar varios casos que son de interés en materia de ciberseguridad, y de los cuales se podrían esperar aportes importantes para el sector académico. Para realizar esta revisión de una manera que no sea aleatoria, se toman nuevamente como base las recomendaciones del BID, que califica como los Estados más avanzados en materia de ciberseguridad a Estados Unidos de América, Estonia, Israel y Corea del Sur (Lewis, 2016). Debido a limitaciones idiomáticas, además de tratarse de países que tienen un tratamiento muy hermético de sus documentos, se debe descartar a Rusia y a China para esta revisión.

Como es de esperarse, los Estados Unidos de América presentan una Estrategia de ciberseguridad que presenta unos lineamientos generales, que además abarca el tema de alianzas internacionales, y al sector académico lo sitúa en el papel de capacitación (Department of Defense, 2015). No obstante, lo interesante en este caso es cómo existen políticas complementarias que abordan la intersectorialidad de la ciberseguridad, incluso provenientes de otros departamentos; ya en el caso del sector académico está la *National Initiative for CybersecurityEducation (NICE)*

*Cybersecurity Workforce Framework* del Departamento de Comercio, en la cual se estipulan las tareas, herramientas y capacidades que se deben desarrollar en pro de este objetivo (Newhouse et al., 2017). Para futuras revisiones, y dado el carácter nacional de este país, se requiere una revisión de las políticas privadas en esta materia y en este sector.

Por otra parte, como es sabido, Estonia fue víctima de uno de los mayores ataques cibernéticos registrados, y por tal motivo la ciberseguridad es prioritaria en su Estrategia Nacional, haciéndola líder en la Unión Europea (Carr, 2011). A raíz de esto, y dada la naturaleza soterrada del ciberespacio, una de las particularidades de la política pública estonia es que tiene una versión pública y otra clasificada; de la primera, parte otra particularidad en que el ministerio encargado de centralizar y coordinar la Estrategia de ciberseguridad en Estonia es el Ministerio de Asuntos Económicos y Comunicaciones, y no el Ministerio de Defensa (Ministry of Economic Affairs and Communication, 2014). Sin embargo, aunque reconocen la necesidad de la participación del sector académico, abiertamente no se le asignan mayores tareas, aunque en este caso la capacitación se da a nivel local e internacional dada la experiencia estonia (Pernik & Tuohy, 2016).

Al observar el caso de Israel, dentro de su política de ciberseguridad presenta un programa educativo específico liderado por el propio Ministerio de Educación, el *Magshimim*, que además involucra a el IDF, la Oficina del Primer Ministro, la Agencia de seguridad israelí, el *Mossad*, la Lotería Estatal Israelí y la Fundación *Rashi* (Housen-Couriel, 2017). Este programa se adoptó como política nacional a partir de 2013 luego de una prueba piloto de dos años, y busca instruir a los estudiantes de últimos años de bachillerato que demuestren aptitudes informáticas y buen desempeño académico para servir en las unidades tecnológicas del IDF (Rashi Foundation, 2018). Entonces, se evidencia aquí cómo el tema de prevención temprana toma un nuevo cariz, y la necesidad de actuar en sinergia con los estamentos de seguridad del Estado para así lograr mejores resultados.

Finalmente, Corea del Sur más que aplicar una política de ciberseguridad, ha diseñado todo un libro blanco aplicado al Internet específica-

mente. Lo novedoso y realmente diferenciador de este documento, es el hecho de que cubre desde la academia la necesidad de impartir una ética del Internet, al cual contempla principalmente protección a menores, y lo hace con programas lúdicos que lleguen a esa población (s.a., 2015). Por ende, los aportes que se pueden dar desde el sector académico van más allá de considerar exclusivamente la capacitación técnica, y requieren del aporte de otros campos de estudio.

Luego de revisar todos estos casos, es claro que al sector académico aún le queda mucho por abarcar en materia de ciberseguridad, como agente proactivo y parte interesada en el desarrollo de este campo. Si bien el sector académico por principio debe encargarse de la capacitación de los agentes de ciberseguridad, como lo demostraron los documentos revisados, también tiene el deber de educar en el buen uso del Internet y los componentes éticos alrededor de este, y desde edades tempranas. De todos modos, queda aún por explorar al sector académico como agente activo en la prevención de ciberataques, dada su participación dentro del ciberespacio, y los nuevos retos que puedan ir surgiendo en el futuro.

## 2. La academia frente a la seguridad digital

En cuanto a la ejecución del papel de la academia como capacitador en seguridad, es interesante notar cómo este lleva a un amplio rango de aspectos que abarcan todos los sectores de la sociedad, conduciendo a un vasto número de publicaciones en seguridad digital. Por esta razón, es que hizo una revisión desde los principales motores de búsqueda de artículos académicos como Scopus, Wiley o Google Scholar para clasificar en categorías amplias los artículos académicos existentes que aborden el tema de Seguridad Digital. Por consiguiente, en este aparte se hará un esbozo de cómo la academia cumple con su papel de capacitador en seguridad digital, y las lecciones que se puedan aprender de estos casos.

Antes de continuar, es pertinente traer a colación los resultados de las mesas de trabajo para la identificación a través de las múltiples partes

interesadas de las líneas de investigación en gestión de riesgos en seguridad digital, desarrolladas en conjunto por MinTIC y la Escuela Superior de Guerra el 26 de abril de 2018. En ellas, dentro de la mesa específica al sector académico se reafirmó una vez más que el papel que debe desempeñar dicho sector es el de capacitador, agregando además la necesidad de crear un centro de innovación en seguridad digital, como también la creación de una red académica en esta materia (Bohórquez-Keeney, 2018). Así, observando esto, el alcance de la academia en seguridad Digital va más allá de la instrucción formal y busca ampliar su acceso de manera multisectorial.

Si bien esas fueron las conclusiones principales de las mesas de trabajo, no se pueden echar en saco roto las demás propuestas presentadas dentro de su realización, puesto que son propuestas de las que se alimentan los artículos académicos reseñados más adelante. En ese orden de ideas, entre las temáticas relevantes avanzadas en la actividad están: Internet de las Cosas, Infraestructura Informática Crítica, Ciberinteligencia y Ética Digital (Bohórquez-Keeney, 2018). De tal modo, estas cuatro temáticas serán los ítems a revisar en esta parte del estado de la cuestión, y así empezar a evidenciar los avances de la academia como capacitador en seguridad Digital.

Al iniciar a un nivel general, es rescatable la publicación hecha por la Escuela Superior de Guerra "General Rafael Reyes Prieto", acerca del ciberespacio a cargo de Andrés Gaitán (2012), en el cual se hace un abordaje general del quinto dominio estratégico. Por supuesto, al ser una producción desde las ciencias militares su enfoque está encuadrado en el tema de ciberguerra, y los alcances que esta ha tenido hasta la fecha de publicación del texto. Este es un referente importante, al tratarse de uno de los primeros textos en Colombia que abordan al ciberespacio, y lo referente a la seguridad dentro de este, desde una perspectiva académica.

De igual manera, no se deben descartar los avances académicos hechos sobre el papel central del sector académico en el tema de seguridad digital, que se estableció anteriormente, es decir, la capacitación en seguridad digital. Bajo esta línea se encuentran trabajos como el presentado por Jiménez *et al*. (2014), en el cual no solo se hace énfasis en la capacita-

ción en seguridad digital, sino que lo hace en la necesidad específica que tiene la academia en apropiarse de estas herramientas, al hacer un estudio de caso en los planteles de educación básica y media en Sogamoso, Boyacá. También relevantes, son los artículos en capacitación académica que abogan por una mayor cercanía entre el sector público y el privado, teniendo en cuenta el alcance que debe tener la seguridad digital, tal como lo argumentan Acosta y Martínez (2017).

Así, entrando ya en los ítems propuestos, una tendencia relevante que se está dando en la actualidad es el *Internet of Things* o Internet de las Cosas, entendido como "el concepto de que todo puede ser enlazado a un aparato conectado a la red para recolectar o hacer uso de datos" En primera instancia, están aquellos documentos que dan una visión general sobre la seguridad en el Internet de las Cosas, así, trabajos como el de Huang *et al.* (2016) investigan las posibles vulnerabilidades dentro de estas redes, y las formas de mitigarlas, o como los de Roman *et al.* (2013) que dan cuenta del alcance multidimensional de este nuevo fenómeno cibernético. Consecuentemente, existen también textos muy completos como el presentado por Tejero (2017), proveyendo metodologías específicas de seguridad en casos puntuales.

Por otra parte, la seguridad en el Internet de las Cosas no se limita exclusivamente a temas técnicos o de ingeniería, debido a su alcance también es un campo fértil para el derecho, las ciencias jurídicas y la ciencia política, campos de conocimiento que tienen algo que decir al respecto. Así pues, Losavio *et al.* (2018) exploran el impacto del Internet de las Cosas en temas como la privacidad y autonomía personal, la toma de decisiones políticas y su elaboración, y los procesos jurídico-legales; haciendo que todo este entramado sea beneficioso para los encargados de desempeñar estas funciones, pero también para aquellos que buscan sacar provecho de las mismas desde la ilegalidad. De esta forma, se demuestra que el tema de la seguridad digital es un tema multidisciplinar, y la importancia de que sea abordado desde los diversos sectores dentro de la academia.

Anteriormente, en el presente documento se trató el tema acerca de la infraestructura informática crítica, y en este instante cobra importancia

resaltar las líneas de investigación que desde la academia han avanzado sobre este tema. Al igual que el Internet de las Cosas, se encuentra la convergencia de varios campos del conocimiento alrededor de este tema, y por supuesto desde la ingeniería ya existen varias propuestas, ejemplo el documento elaborado por García Font *et al*. (2014) que estudia el vínculo entre las plataformas *Smart City* y la infraestructura crítica, y los potenciales fallos en cascada que se pueden dar a causa de esta. Como es de esperarse, las ciencias militares también hacen aportes importantes frente al estudio de la seguridad Digital en la Infraestructura Crítica, así Giudici (2013) establece la importancia entre la seguridad Digital y la Infraestructura Crítica como teatro de operaciones.

Es más, las ciencias sociales no se ven limitadas en este aspecto de la seguridad Digital, por el contrario, dentro de sus distintas disciplinas se pueden encontrar aportes interesantes que proveen de otras perspectivas. Por ejemplo, desde la economía se estudia la dependencia de la Infraestructura Crítica hacia las nuevas tecnologías digitales, y cómo esta puede afectar la adecuada administración de los recursos (Kepchar, 2016). La antropología también se ha manifestado al respecto, ideando aprovechar estas infraestructuras digitales para el avance del desarrollo académico en las sociedades (Kenner, 2014).

En cuanto a la ciberinteligencia, se pueden determinar dos corrientes importantes abordadas desde la academia: las responsabilidades de las entidades estatales encargadas de este tema, y la importancia de la *deep web* o red profunda, y en especial dentro de esta, la *dark web* o red oscura en este tipo de actividades. En primer lugar, Eom (2014) hace una propuesta desde una perspectiva operacional, en donde los roles deben ser asignados según las fases de una operación, y al tratarse de este nivel estratégico, se coordina lo táctico, lo estratégico y las políticas públicas alrededor de las acciones. Por su parte, Martín (2016) establece la ciberinteligencia como una responsabilidad de las instituciones tanto públicas como privadas, y hace un llamado para hacer el paso definitivo de una posición reactiva en el ciberespacio, a una proactiva.

En segundo lugar, y del mismo modo, también Martín (2017) hace referencia a la vasta cantidad de información existente dentro de la *deep*

*web* y la *dark web* referente a amenazas, vulnerabilidades y riesgos, recordando que la materia prima de la Inteligencia es precisamente la información. Asimismo, también se encuentran documentos que no solo definen de manera precisa lo que es la *dark web*, sino que además hacen una clasificación y taxonomía de las herramientas de tecnología y herramientas de acceso y monitoreo a este sector del ciberespacio, de modo que puedan ser aprovechadas para avanzar en temas de Inteligencia, y encontrar los vacíos de investigación en este campo (Fachkha & Debbabi, 2016). Como se puede evidenciar, dentro de la ciberinteligencia la academia tiene un amplio campo de acción por recorrer, dando una luz promisoria a las investigaciones que se adelanten sobre este tema.

Otro campo de estudio importante, y que a veces puede ser subestimado, es el tema de la ética en el ciberespacio, que por su naturaleza particular es claramente un tema interdisciplinar, siendo la ética un tema de amplio rango y cuyo estudio parte de la misma filosofía. Ejemplo de esto, son las obras que buscan dilucidar a quién debe atribuírsele la responsabilidad por fallas cibernéticas que pueden acarrear situaciones lesivas a usuarios y/o sistemas, como lo plantea Dennett (2014) con su elocuente título *"When HAL kills, who's to blame?: computer ethics"*. Ya más puntualmente, un sector importante para la ética ciberespacial es la administración pública, como lo señala Kernaghan (2014) con los cambios éticos que traen las TIC para los servidores públicos en el cumplimiento de sus labores, o cómo la ética es una consideración importante en las plataformas de *Smart City* e Internet de las cosas (Losavio et al., 2018).

Desde otra perspectiva, la ética cibernética también tiene aportes importantes para su propia fuente de producción, es decir, cuáles deben ser las aproximaciones éticas de la academia en esta era de expansión digital, y en especial en sus actividades específicas. Es así, que por un lado, se encuentran textos que plantean los nuevos retos éticos a los que se enfrentan los educadores en su labor, gracias a la aparición del Internet y las TIC y su importante influencia en el sector educativo (Olcott *et al.*, 2015). Por otro lado, también es de especial atención los cuestionamientos éticos que trae consigo la investigación, aún más si se

consideran nuevos procedimientos como el *big data*, al poderse infringir el derecho a la privacidad de las personas, tomando datos que en principio son personales pero se encuentran en el ciberespacio, sumado al hecho de que la investigación académica es de tipo público (Sula, 2016).

De este modo, se han cubierto los aspectos realzados en la mesa de trabajo mencionada como los más importantes a cubrir e investigar por parte de la academia colombiana, pero esto no significa que sean los únicos relevantes. Por ejemplo, una vez más las ciencias sociales señalan los importantes cambios que trae la seguridad Digital, como se observa desde la sociología política y los retos que afronta la gobernabilidad de las sociedades gracias a la aparición del ciberespacio (Eijkman, 2014); en efecto, hoy en día que el concepto de seguridad abarca mucho más que la Defensa del Estado, este tipo de avances académicos son una contribución importante. Por ese motivo, es que autores como Sancho (2017) que evidencian las facilidades para la gobernabilidad que provee el ciberespacio, pero también los riesgos que se enfrentan dentro del mismo, máxime de su capacidad de llegar hasta toda, o casi toda, la ciudadanía.

Otro aspecto importante para tener en cuenta desde la academia es lo pertinente con el derecho del ciberespacio, o cómo las situaciones generadas por este deben ser reglamentadas o reguladas, ya que han sido ampliamente referenciados los retos legales desde el advenimiento del Internet frente a temas tales como derechos de autor, pornografía, datos personales, etc. En consecuencia, se encuentran libros completos que cubren todos estos distintos aspectos legales y los nuevos retos que se les presentan desde el ciberespacio, como el que lleva la autoría de Kosseff (2017), que cubre un amplio rango de temas, desde protección de datos, litigios, y sociedades público-privadas; pasando por *hacking*, monitoreo, ciberseguridad y otros temas propios del ciberespacio; hasta llegar a temas de gobierno y Derecho Internacional. Este último aspecto, el Derecho Internacional, es de vital importancia puesto que, al trascender fronteras, el ciberespacio logra imponer nuevos desafíos a las relaciones entre Estados y demás actores internacionales (Segura, 2017).

Llegado a este punto, se ha podido revisar cuáles son los principales temas a abordar en el presente por parte de la academia respecto a

seguridad digital, y se ha podido constatar que todavía existe un amplio campo por investigar. De modo que, siguiendo las propuestas hechas por los mismos académicos, se ha podido verificar la importancia de revisar desde este sector temas como Internet de las Cosas, infraestructura informática crítica, ciberinteligencia y ética digital, además de notar otros temas dignos de mención dentro de la seguridad digital como la gobernabilidad digital y el derecho en ciberespacio. Solo en estos temas, el interesado en llevar a cabo una investigación académica en uno de ellos encontrará mucha tela por cortar.

A pesar de esto, no se puede asegurar que el campo de acción de la academia esté limitado a estos temas, o que la anterior haya sido una lista totalmente omnicomprensiva, y todavía quedan temas por revisar más adelante. Así entonces, en el siguiente apartado se hará una revisión de los retos futuros de la academia en materia de seguridad digital, si bien no siempre puede haber plena certeza de lo que depara el futuro, es posible mirar las tendencias que se han venido generando y en sus posibles consecuencias. Precisamente, es esto lo que se revisará a continuación.

## 3. Ciberseguridad y académica hacia el futuro

Una vez revisados los alcances y las funciones del sector académico en cuanto a ciberseguridad, queda preguntarse cuál va a ser la proyección a futuro en este campo, y qué novedades vendrán consigo. Lo interesante de esta mirada prospectiva es que, al darse los avances en ciberespacio de una manera rápida y vertiginosa, los ítems aludidos en la sección anterior bien podrían considerarse como el futuro del ciberespacio, a la vez que su presente, y muy posiblemente al leerse estas líneas, su pasado. Por ello mismo, se hace necesario reconocer a tiempo las nuevas tendencias que se proyectan y presentan en lapsos de tiempos futuros.

Para lograr tal cometido, se tomará como referencia el documento elaborado por la empresa ESET (2018), debido a su pertinencia y actualidad, frente a otros documentos elaborados por empresas de seguridad Digital cuyas proyecciones se hicieron en años anteriores. Así, siguiendo

esta directriz, los temas considerados de relevancia futura son a saber: *ransomware*, ataques a Infraestructura Crítica, investigación policial de *malware*, *hackeos* a la democracia, y datos personales (ESET, 2018). Así pues, en este aparte se revisarán los aportes de la academia a los ítems referenciados, como también a aquellos que puedan surgir de la revisión de estos.

En el primer caso, el *ransomware* es definido como el *software* malicioso que niega el acceso a unos datos o información hasta que se pague un rescate (Alessandrini, 2016), de ahí su nombre. Por su parte, investigando sobre los avances académicos más recientes hechos al respecto, es curioso notar los contrastes entre lo escrito por la academia hispanoparlante y lo elaborado por la academia angloparlante, dado que los primeros todavía se concentran en casos bastantes específicos como lo fue el caso Wanna Cry (Martínez & Hernández, 2017). O de forma un poco más general, se estudia el comportamiento del *ransomware* en dispositivos más específicos, como por ejemplo los dispositivos Android (Sánchez, 2018).

Así mismo, en el caso angloparlante, lo que se estudia respecto al *ransomware* va más orientado hacia temas de prevención tanto a nivel técnico como social, como lo es la detección temprana de este tipo de *software* malicioso usando características de tráfico HTTP (Cabaj *et al*., 2018). En cuanto al aspecto social, se encuentran trabajos que abordan la prevención ante este tipo de amenazas en la detección de posible ingeniería social tan común en estos casos (Thomas, 2018), en particular, en los casos de empleados públicos o de empresas privadas, que es donde son más frecuentes este tipo de ataques. Por lo tanto, es claro que las necesidades y vulnerabilidades frente al tema del *ransomware* varían dependiendo de la ubicación geográfica, y más puntualmente, el nivel de dependencia que se tiene del ciberespacio, o su precariedad.

En ese sentido, trayendo nuevamente a colación el tema de la infraestructura crítica, pero ahora concentrándose en el tema de ciberataques hacia la misma, es visible cómo este campo muestra ese vínculo entre presente y futuro mencionado al inicio de este aparte. Por supuesto, ya se encuentran en el mercado libros especializados sobre la protección de la

infraestructura crítica de ataques provenientes del ciberespacio, y su abordaje es omnicomprensivo yendo desde las macroestructuras hasta los aparatos personales, que es el ejemplo del *Handbook on Securing Cyber-Physical Critical Infrastructure (Das et al., 2012)*. De igual manera, se encuentran documentos que idean mecanismos de valoración de ataques cibernéticos a infraestructuras críticas (Genge *et al*., 2015), o bien que se delimitan a la protección de elementos específicos de la Infraestructura Crítica, como lo son los recursos energéticos (Correa-Henao y Yusta-Loyo, 2013).

Es de destacar, el hecho que en la región suramericana se adelanten trabajos que buscan la protección de la Infraestructura Crítica de sus respectivos Estados, lo cual puede ocupar los vacíos evidenciados en la primera sección de este capítulo. Como es de esperarse, Brasil hace un interesante aporte desde la academia a la seguridad digital de su infraestructura, presentándola como un imperativo de su gran estrategia, y como soporte de sus metas como potencia regional (Amaral, 2014). Pero si se trata de llenar vacíos temáticos, es interesante el planteamiento que hacen Robert Vargas *et al.* (2017) al proyectar una visión político-estratégica de la seguridad digital de la infraestructura crítica ecuatoriana, resolviendo así el aporte de la academia de su país a ese tema.

A otro nivel, tomando en consideración la seguridad digital de la ciudadanía se torna evidente la necesidad de vincular los procesos policivos y jurídicos con la investigación sobre *malware*, donde se encuentran nuevamente puntos de intersección entre la ingeniería y las humanidades, específicamente los estudios en derecho. Por un lado, desde el derecho, se tienen las investigaciones hechas respecto a los procesos que deben llevarse a cabo para la investigación y enjuiciamiento por la producción de este tipo de *software*, lo cual a hoy en día sigue siendo difícil de rastrear y legislar (Rayón y Gómez, 2014). Por otro lado, desde la ingeniería, se hacen estudios prospectivos sobre el futuro del *malware*, como es el caso del artículo elaborado por Pathak & Nanded (2016), donde se perfila el *ransomware* como tendencia criminal a seguir, confirmando lo escrito anteriormente.

De estas tendencias, la más marcada encontrada en esta investigación es el tema de la informática forense, que también contiene así aporte

de los campos académicos mencionados. Así, por el lado del derecho se contemplan los dilemas técnicos, legales y éticos que se presentan al llevar a cabo esta actividad, en espacial, en un tema de actualidad y futuro en temas ciberespaciales, como lo es la nube informática, cuyas características virtuales hacen estas delimitaciones más difusas (Broucek & Turner, 2013). En cuanto a la ingeniería, lo que se explora dentro de este campo académico es precisamente cómo las nuevas tecnologías pueden mejorar o entorpecer estos procesos forenses, y los impactos que pueden tener en cuanto a la investigación policial (Piccirilli, 2016).

Ahora bien, cambiando de tema, y considerando cuándo lo ciudadano impacta lo político, demostrando en cierta medida cómo el ciberespacio debe entenderse desde el nivel operacional, los *hackeos* a la democracia son una de las amenazas presentes que dominan la agenda. Una buena muestra de esto es el artículo desarrollado por el trabajo conjunto realizado por varios profesores doctorales de las ciencias sociales provenientes de academias prestigiosas, tales como la Harvard Kennedy School o la King's College, donde se plantean cuestionamientos importantes a raíz de los recientes ataques digitales al proceso electoral estadounidense, poniendo sobre la mesa si este tipo de procesos deben ser considerados parte de la Infraestructura crítica (Shackelford *et al.*, 2017). Así, resaltando lo dicho, se encuentra el trabajo de Torres-Soriano (2017) "Hackeando la democracia: operaciones de influencia en el ciberespacio", en donde se valoran los impactos electorales desde las acciones en el ciberespacio.

Pero el análisis del *hackeo* a la democracia no se limita a las amenazas externas, sino que también se evalúa cómo el mismo proceso desde su interior puede ser sujeto a explotaciones por parte de *hackers* o a fallas masivas (Yasunaga, 2017). Del mismo modo, también se deben considerar aquellos procesos distintos a las votaciones que son igualmente importantes para un sistema político democrático; se toma por caso la reflexión hecha por Benítez (2013) acerca de la promoción de la democracia en el ciberespacio, vista a través del lente de la movilización social, y qué tantas garantías hay de que esta se dé. Como puede evidenciarse, la relación entre seguridad Digital y democracia es todo un campo de

análisis el cual debe ser abordado por la academia, y que marca pauta para investigaciones futuras en las múltiples aristas que este tiene.

Un ítem que claramente refleja esa interacción entre pasado, presente y futuro de la seguridad digital, es el tema de la protección de datos personales, demostrando ser un tema recurrente que en cada momento presenta nuevos retos. Siguiendo esta línea, el problema ya no se centra exclusivamente en el acceso de estos grandes datos o *big data* disponibles en el ciberespacio, ahora está también el dilema de cuál debe ser el uso adecuado de estos datos, ya que este uso contempla varios riesgos para las empresas y el tercer sector (Tascón, 2013). Asimismo, una prueba fractal de las interconexiones generadas por este, el quinto campo estratégico, son los estudios llevados a cabo sobre los grandes datos recolectados a través del Internet de las Cosas, el cual se revisó en este texto en el aparte anterior, el cual ya cuenta con sus propios estados de la cuestión (Chen *et al*., 2015).

Aun con estos avances y nuevos alcances de los estudios alrededor de los datos personales, dichos estudios no se limitan exclusivamente a su protección y uso, nuevos retos aparecen que se pueden vincular a otros temas anteriormente revisados como la ciberinteligencia. Uno de estos nuevos retos, consiste en que además de la protección y uso de grandes datos y datos personales existe también el riesgo de que estos sean falsos, y la ausencia de veracidad de estos datos puede conducir a lecturas erradas sumando a confusiones y estimaciones equivocadas (Lu *et al.*, 2014). Fuera de esto, es de primordial interés un libro desde el derecho como el redactado por Garriga (2016), cuyos señalamientos hacia el *big data* van desde la dignidad ciudadana y el derecho a la intimidad, hasta la protección de datos dentro y fuera de las fronteras.

En suma, en este aparte se ha podido revisar cómo algunas tendencias en seguridad digital no solo se han mantenido desde el auge del ciberespacio, sino que se mantienen en el presente, e incluso proyectan nuevos retos en el futuro previsible. Tal es el caso de temas ya antes abordados en este capítulo, como es el caso de la protección digital de la infraestructura crítica, el *malware*, y la protección de datos personales; a medida que avanza la tecnología digital, estos ítems toman

nuevas facetas, y el sector académico no puede quedar rezagado ante estas, como acá se ha probado. Similarmente, aparecen nuevas tendencias que pueden tener una semilla en el pasado, pero en el presente y a futuro han cobrado vida propia, como lo son el *ransomware* y los *hackeos* a la democracia, que ya no pueden considerarse parte del conjunto general de *malware* o *hackeo*, ya que sus características les han otorgado una naturaleza particular que debe ser estudiada con sumo cuidado.

Con estas consideraciones, ya se puede vislumbrar el papel del sector académico frente a la seguridad digital, y los importantes aportes que puede dar al Estado, la economía, y principalmente, a la sociedad en general. Quizás, queden ítems y temas por considerar, o puedan aparecer nuevos campos por estimar de los que aún no hayan sido detectados, esto entendiendo que las miradas a futuro, incluso las más precisas, son especulativas; no obstante, esta primera mirada proveerá los caminos para futuras investigaciones, y como se ha visto, la interconectividad es tal que se pueden vislumbrar los futuros retos con esta exploración. Lo anteriormente expuesto será, pues, insumo para la revisión de los principales hallazgos, esperando resulte de insumo para a las mencionadas investigaciones.

## Conclusiones y hallazgos

A lo largo de este capítulo, se han revisado los alcances del sector académico frente al tema de la seguridad digital, tanto el papel que debe desempeñar como parte de la infraestructura crítica del Estado, como su importante función social dentro de este. En los documentos revisados, se observaron las distintas tendencias actuales y futuras de los retos que enfrenta la academia frente al tema de seguridad digital, sumado a su participación en las políticas públicas elaboradas con el fin de abordar este tema. Por ello, a continuación, se presentarán los principales aportes hechos en esta revisión documental, como también algunas observaciones al respecto para el fomento de nuevas ideas.

A grandes rasgos, la primera conclusión que se puede extraer es el hecho de que la principal función del sector académico, en cuanto a

políticas públicas de seguridad digital, es cumplir la función de formador y capacitador en este tema, lo que queda aún por verse es el alcance de dicha capacitación. La segunda gran conclusión que se puede extraer es la importancia que posee la infraestructura crítica para la seguridad digital, y cómo este es un aspecto muy a tener en cuenta en cualquier investigación académica sobre el campo, al tener múltiples alcances, riesgos y amenazas. Finalmente, la tercera gran conclusión es la existencia a gran escala de los varios cambios sociales y jurídicos que trae el ciberespacio, y puntualmente, la seguridad digital, que deben ser contemplados en este tipo de investigaciones.

Mientras tanto, es bastante claro que el papel principal del sector académico en materia de seguridad digital es el de formador y capacitador, sin embargo, al revisar las políticas públicas, no resulta tan claro su alcance. De entrada, no es del todo claro desde qué nivel se debe comenzar con esta instrucción, algunas de las políticas públicas revisadas como la israelita o la surcoreana proponen un inicio temprano en este tipo de formación, iniciando desde la misma primaria como semillero o como protección a menores, y otras proponen su implementación desde la Educación Superior. Sumado a esto, en muchas de estas políticas no se establecen delineamientos claros de la instrucción a impartir, y los objetivos específicos o metas claras a lograr con ella.

Una vez establecidas estas metas, también queda por aclarar, dada la naturaleza del ciberespacio que difumina los límites entre lo público y lo privado, qué tanta incidencia debe tener el uno o el otro en las capacitaciones del sector académico. Aquí, cobra relevancia lo explicado por Roth (2002) en los modelos mixtos de políticas públicas, ya que las políticas públicas de seguridad digital abordan un tema de alto interés público, como lo es la infraestructura crítica del Estado, pero el sector académico se encuentra conformado por varias instituciones privadas que a su vez cumplen una función social; por lo cual, cabe proyectar la idea de que "las políticas públicas ya no se conciben como el resultado de una competición entre grupos … sino como el fruto de la negociación entre el Estado y los representantes de los grupos sectoriales involucrados" (p. 33). Ejemplo de esto, fueron las políticas revisadas de Estonia

y Estados Unidos, que dan margen de independencia a las instituciones privadas sin que olviden su función ante la sociedad.

En adición a esto, otra consideración que salió a flote en esta revisión documental es el contenido mismo de dicha formación y capacitación, del cual se partió para hacer la posterior revisión en los dos siguientes apartes. Por un lado, aunque pueda parecer obvio, se encuentra la capacitación en seguridad digital desde el enfoque técnico y de la ingeniería, y muchas de las políticas públicas revisadas apuntan hacia este aspecto, justificado por la renovación constante de las amenazas que provienen del ciberespacio, que aprovechan el mayor número de interconexiones que se dan cada día. Por otro lado, algunas de estas políticas hacían también énfasis en la parte social y humanística de la seguridad Digital, al tratar la necesidad de un entramado legal para poder llevar a cabo las acciones necesarias, como también la necesidad de llevar a cabo programas de ética digital y buenas prácticas en el ciberespacio.

En virtud de lo anterior, retomando entonces el segundo eje del presente estado de la cuestión, en cómo ejecuta sus acciones el sector académico en cuanto a capacitación sobre seguridad digital, se recuperaron algunos trabajos ya existentes sobre dicho procedimiento, como también las principales tendencias que deben guiar las investigaciones al respecto. De esta manera, se visibilizó el trabajo en curso que lleva a cabo la Escuela Superior de Guerra "General Rafael Reyes Prieto", en cuanto a ciberespacio y seguridad digital, no solo por el hecho de poseer ya en su bibliografía publicaciones al respecto, sino también por el trabajo en curso que se está efectuando en la materia, y del cual este capítulo hace parte. Así mismo, se revisaron proyectos que se aproximan a casos puntuales y buscan aportar nuevas visiones y soluciones a los problemas inherentes a la seguridad digital, o aquellos que buscan integrar a las partes interesadas en este tema para poder adelantar acciones conjuntas de mayor impacto y alcance.

Agregado a esto, la interconectividad del ciberespacio se pudo reflejar en los temas propuestos en la mesa de trabajo, al no tratarse del todo de ítems separados entre sí, sino que se traslapan el uno al otro en temas de seguridad digital. Por ejemplo, el tema del Internet de las Cosas hace

que haya nuevas conexiones y una mayor multiplicidad de efectos de cascada, los cuales pueden afectar la infraestructura informática crítica cuya prioridad ha sido transversal al estudio realizado en estas páginas, ya que de su protección depende el normal funcionamiento del Estado. Análogamente, desde la ciberinteligencia se deben estudiar los alcances de la *deep web*, y más que todo de la *dark web*, para encontrar los patrones y trazas de posibles amenazas hacia la infraestructura crítica y la ciudadanía, pero esto no nos debe alejar de la ética y buenas prácticas, que también se han recalcado como tema transversal.

No obstante, los temas propuestos por la mesa de trabajo no son los únicos relevantes para el sector académico en su papel dentro de la seguridad digital, en este trabajo también surgieron otras propuestas que se salen un poco del esquema mental en este tema. En este punto, se debe contemplar el concepto de seguridad más allá de su acepción tradicional como la protección ante unas amenazas físicas, sino también como la manutención de la estabilidad a futuro (Buzan & Hansen, 2009); de ahí, la importancia del derecho tanto nacional como internacional, como el aporte que puedan brindar ciencias sociales como la ciencia política, para la manutención de la gobernabilidad digital y los impactos sociales provenientes del ciberespacio. Todo esto, simplemente demuestra cómo este, el tema de la seguridad digital es interdisciplinar y transdisciplinar, y qué mejor sector para abordar un tema así que la academia.

Con estos postulados, ya es posible dar una mirada hacia el futuro respecto al papel del sector académico y la seguridad digital, lo cual fue la temática del tercer aparte de este capítulo, y como se observó, es un tema que abarca simultáneamente pasado, presente y futuro. Nuevamente, se hallaron temas que en principio parecen ser temas aparte con solo la seguridad digital como eje común, pero que nuevamente se puede notar una interconexión y una interdependencia entre ellos, evidenciada dentro del aparte con la interacción Estado-Infraestructura Crítica-sociedad. Así, subrayando una vez más, la importancia de la interdisciplinaridad que el sector académico puede aportar para estos casos, y así poder integrar distintas disciplinas y distintos niveles.

En efecto, el estudio de *ransomware*, ataques a infraestructura crítica, investigación policial de *malware*, *hackeos* a la democracia, y datos personales, marca la pauta a seguir para el sector académico en investigaciones presentes y futuras. En este instante, fue posible vislumbrar cómo la infraestructura crítica no es un concepto estático, sino que también plantea que los procesos democráticos hacen parte de esta, debido a la importancia que en ellos recae y las vulnerabilidades que estos tienen de cara al ciberespacio, lo cual ya ha empezado a salir a la luz pública. De igual manera, en el caso suramericano se puede observar cómo la protección de la infraestructura crítica es una herramienta de vital importancia para la proyección regional e internacional.

En cuanto a los otros dos ítems, estos también demostraron tener interconectividad entre sí y los dos anteriores, además de hacer la meta-referencia propia de este caso en donde también se interconectan disciplinas y sectores sociales. Tanto en el estudio y detección del *ransomware*, el *software* malicioso que secuestra información a cambio de un rescate, como en la colaboración entre Policía y empresa privada en la investigación de *malware*, se denota la amplitud de estos campos, y cómo se requiere de la colaboración de las varias partes interesadas para llegar a un resultado exitoso. De nuevo, se tiene ante sí la necesidad de una visión integradora para enfrentar los nuevos retos, que solo el sector académico puede proveer.

Con todo esto, es claro que hay mucho por recorrer en materia de seguridad digital y el sector académico en su papel de capacitador y formador no puede quedarse por fuera de cualquier política pública al respecto. Esto solo es posible si se tiene en cuenta que el ciberespacio va más allá de una simple red de computadores y aparatos interconectados, y se miden los impactos de los usuarios detrás de ellos, que son precisamente los que aprovechan este nivel estratégico, ya sea en beneficio de la sociedad y el Estado, o en su detrimento.

En este capítulo, se proveyeron los primeros lineamientos para futuras investigaciones y nuevos desarrollos en materia de seguridad digital, buscando así una mejora de las condiciones de Colombia y su ciberes-

pacio. Por ello, se resaltó la importancia del sector académico como faro que debe guiar los procesos que se lleven a cabo a todo nivel, vinculando lo estratégico del Estado, con lo particular de lo ciudadano y lo empresarial. Es así, que la academia es la luz que guía a la seguridad digital en el caos virtual.