La importancia del componente educativo en toda estrategia de Ciberseguridad[1]

Juan Cayón Peña[2]
Luis A. García Segura[3]

Recibido:
1 de septiembre de 2014

Aprobado:
18 de diciembre de 2014

Resumen

Este artículo pretende estudiar las principales Estrategias de ciberseguridad publicadas hasta el momento, prestando especial atención al componente educativo de las mismas. A partir de este análisis hacemos una serie de recomendaciones de cara al diseño e implementación de acciones educativas relativas a la ciberseguridad. Concluimos que la coordinación entre el sector público y privado, entre los estamentos militares y de los cuerpos de seguridad de un lado y la sociedad civil a la que sirven de otro, es vital para el desarrollo e impartición de un currículo apropiado sobre ciberseguridad en todos los niveles educativos.

Palabras claves:
Ciberseguridad, estrategia, educación, derecho.

Abstract

This article seeks to study the most relevant Cybersecurity strategies published up to this moment, with a special interest in the education component these strategies. Upon this analysis, we suggest a series of recommendations in order for the correct design and implementation of educational Cybersecurity actions and projects. We conclude that the coordination between the private and public sector, military and security forces is vital in order to develop an appropriate Cybersecurity curriculum on all levels.

Key Words :
Cybersecurity, strategy, education, law.

1. Artículo vinculado al grupo de investigación EMERGE de la Universidad de Nebrija, España.
2. Doctorado en Derecho de la Universidad Pontificia Comillas ICADE. Licenciado en Derecho y Graduado Superior en Ciencias Jurídicas por la Universidad Pontificia Comillas ICADE. Rector de la Universidad Nebrija y miembro del grupo de investigación EMERGE. Es Académico Correspondiente de la Real Academia de Jurisprudencia y Legislación (Madrid, España). Correo electrónico: jcayon@nebrija.es
3. Doctorando en Derecho de la Universidad Nebrija. Magister en Derecho Empresarial por la Universidad Nebrija. Licenciado en Derecho por la Pontificia Universidad Católica Madre y Maestra de Santo Domingo. Es abogado ejerciente del Ilustre Colegio de Abogados de Madrid -ICAM-, miembro académico de la American Bar Association (ABA) de Estados Unidos de América y miembro del grupo de investigación EMERGE. Correo electrónico: lgarcise@nebrija.es

Las estrategias de Ciberseguridad

A medida que la tecnología avanza, tanto el sector público como el sector privado dependen cada vez más de sistemas informáticos para llevar a cabo sus operaciones esenciales, especialmente las relacionadas con el capital intelectual y la prestación de servicios de todo tipo (US Government Accountability Office, 2012). Desde la revolución industrial y, de manera especialmente acelerada, desde la irrupción de la sociedad del conocimiento en el último tercio del siglo XX dicha dependencia tecnológica ha supuesto un creciente número de retos jurídicos y sociales, muchos de los cuales aún se encuentran en vías de solución.

A estos efectos, la protección de los sistemas informáticos considerados críticos se ha convertido en un tema de interés nacional, ya que el daño a los mismos puede causar graves trastornos al funcionamiento de cualquier sociedad. Esta es una de las principales razones por las cuales la ciberseguridad es considerada ya como un eje estratégico a nivel nacional que afecta todos los niveles de la sociedad (European Network and Information Security Agency, 2012), y en el que con frecuencia se ven involucrados tanto el sector público como el privado.

La Unión Internacional de Telecomunicaciones proporcionó en el año 2010 la siguiente definición de ciberseguridad, la cual encaja a nuestro entender perfectamente con la esencia de cualquier estrategia nacional:

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciber entorno. (Unión Internacional de Telecomunicaciones, 2010)

Llevado a un plano nacional, la organización a que se refiere la definición anterior sería el total de los sistemas informáticos conectados, junto con los usuarios, pertenecientes tanto a las empresas privadas como a las organizaciones estatales. De ahí que la estrecha colaboración entre sectores sea absolutamente imprescindible para el buen despliegue de la estrategia elegida, como lo es la cooperación internacional ante amenazas que no conocen de fronteras.

Sólo a través de iniciativas que abarquen sectores transversalmente a nivel nacional y, en algunos casos, incluso a nivel internacional, puede una nación o bloque de naciones reducir las amenazas a las cuales están expuestas en el ciberespacio.[4] En este dominio por tanto, las líneas divisorias tradicionales entre lo militar y lo civil, lo público y lo privado, no son tan claras, de ahí que la seguridad nacional se puede ver afectada por un ataque cibernético de gran escala a una empresa u organización privada (Ministry of Security and Justice, 2011).[5]

Un caso reciente que sirve de ejemplo es el ataque sufrido por la empresa Sony Pictures[6] en noviembre del año 2014. Este ataque consistió básicamente en la infiltración de los sistemas y servidores informáticos de la empresa y la posterior circulación en internet de una serie de archivos con

4. Sobre la cooperación entre sectores transversales, ver el artículo de Backstrom y Henderson (2012) titulado "Surgimiento de nuevas capacidades de combate: los avances tecnológicos contemporáneos y los desafíos jurídicos y técnicos que plantea el examen previsto en el artículo 36 del Protocolo I". En el mismo estos autores afirman que dada la creciente complejidad de los sistemas de armas, entre las cuales se encuentran las llamadas ciberarmas, exige que el examen de la licitud de las armas previsto en el artículo 36 del Protocolo adicional I a los Convenios de Ginebra se lleve a cabo de manera interdisciplinaria. En relación con este mismo artículo, Rappert, Moyes Crowe et al (2012) en su artículo titulado "The roles of civil society in the development of standards around new weapons and other technologies of warfare", evalúan de forma positiva el rol que la sociedad civil tiene actualmente en el desarrollo de los nuevos estándares de armas, en contraste con el de los estados.
5. Resulta relevante alcanzar a comprender adecuadamente la noción de Infraestructura crítica manejado en los distintos entornos (anglosajón o continental europeo) que, si bien se refieren a realidades conceptuales distintas, se asemejan en muchos de sus contenidos.
6. Un recuento completo del ataque lo podemos leer en las siguientes direcciones: http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/ y http://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story/

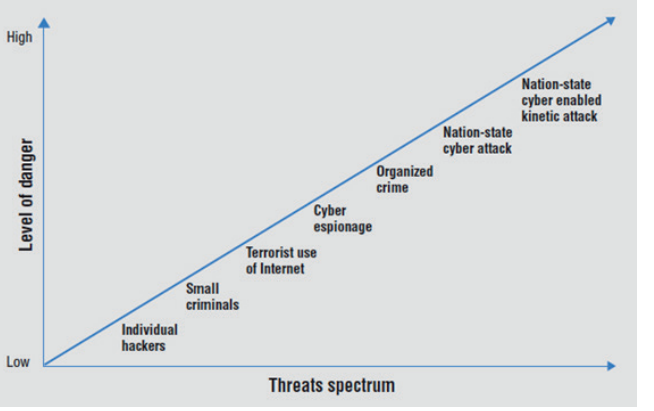
información privada, que contenían, entre otras cosas, correos electrónicos de los principales ejecutivos de la empresa. Dada la sofisticación y magnitud del ataque, el propio presidente de los Estados Unidos de América se pronunció al respecto, indicando que se investigaría a fondo el caso, al tiempo que se deberían mejorar las leyes que protejan a las empresas privadas contra ataques informáticos de este nivel.[7] La importancia de este ataque además viene determinada no sólo por su sofisticación, sino porque incluso llevó a la cancelación del estreno previsto de una determinada película, vulnerando de facto con ello la libertad de expresión entendida como uno de los derechos fundamentales más especialmente protegidos en Occidente.

La propuesta del presidente Barack Obama es una reforma legislativa a nivel federal con el objetivo de facilitar el intercambio de información relativa a la ciberseguridad entre entidades privadas y organismos estatales, para de esta forma proteger mejor a todos los sistemas informáticos y tener una mejor respuesta ante un ataque cibernético (White House, s.f.).

Si bien es cierto que este ataque no vulneró ninguna de las infraestructuras críticas de Estados Unidos de América en la conceptualización europea, bien puede entenderse que sí lo hizo en la conceptualización norteamericana, demostrando la vulnerabilidad de un sector económico, cultural e ideológico en el cual dicho país es líder a nivel mundial: la industria cinematográfica.[8]

Como es sabido y bien se evidencia en el siguiente gráfico, las amenazas a las que las naciones están expuestas en el ciberespacio pueden tener orígenes muy variados y suponer muy distintos niveles de gravedad,[9] al originarse desde el más bajo nivel de persona o personas con el sencillo interés de demostrarse a sí mismos un cierto conocimiento o una capacidad operativa, hasta el más alto en el que ya se involucran estructuras estatales especialmente creadas al efecto y se despliegan sus efectos al mundo real a través de consecuencias materiales que transforman el entorno físico:[10]

Figura 1.



Fuente: (Baldwin & Palfreyman, 2009, p. 5).

Para responder globalmente a todas estas amenazas, los países procuran diseñar e implementar lo que conocemos como una Estrategia de Ciberseguridad (EC). Según la European Union Agency for Network and Information Security (2012), una EC es una herramienta que mejora la seguridad y resistencia de las infraestructuras nacionales de información y servicios de un país. Es un proyecto de alto nivel y jerarquizado, el cual establece una serie de objetivos y prioridades nacionales respecto a la ciberseguridad, las cuales deben cumplirse en un período de tiempo determinado.

De forma similar, el National Security Framework Manual (Klimburg, 2012), define a una EC como la implementación estratégica de una serie de medidas y principios que aseguren la protección de los sistemas informáticos públicos y privados, incluyendo el contenido asociado a los mismos, siempre y cuando tengan relación directa con la seguridad nacional de un país.

7. Para ver un relato cronológico del ataque, ver las siguientes noticias al respecto: http://www.nytimes.com/2015/01/14/us/obama-to-announce-new-cyberattack-protections.html?_r=0 y http://www.businessweek.com/news/2015-01-16/obama-cameron-cybersecurity-agenda-shaped-by-paris-sony-attacks
8. Según ejecutivos de Sony Pictures, el daño económico causado a la empresa sería de mínimo USD $100, 000,000 (Shaw, 2014).
9. Lin (2012) argumenta que hemos visto hasta la fecha solamente una pequeña fracción de todas las posibilidades o situaciones que se pueden dar entorno a los ciberconflictos y el Derecho Internacional Humanitario.
10. Droege (2012), al analizar los conflictos cibernéticos y su relación con el Derecho internacional humanitario, concluye que las operaciones militares llevadas a cabo a través del ciberespacio (ciberoperaciones) conllevarán nuevos medios y nuevos métodos de combate, los cuales hasta el momento no han sido comprendidos adecuadamente. En este sentido, el despliegue militar de ciertas herramientas informáticas representa serios retos a la aplicación de las normas del Derecho Internacional Humanitario.

La implementación y consecuente mejora de una EC incorpora una serie de elementos políticos, jurídicos y administrativos dentro del país que la desarrolla. Estos elementos a su vez requieren de la cooperación, educación y entrenamiento de los principales actores involucrados. Se observa a continuación como es abordado el componente educativo en algunas de las principales EC a nivel global.

El componente educativo

La Unión Internacional de Telecomunicaciones (2007) resalta la importancia que tiene la educación, formación y sensibilización de todos los actores que intervienen en la ciberseguridad:

> Es importante concienciar a todos los que intervienen en el mundo de Internet en cuanto a los beneficios del control de la seguridad y de las medidas elementales que, enunciadas con claridad, definidas y aplicadas inteligentemente, refuerzan la confianza de los usuarios en las tecnologías de tratamiento de la información y de la comunicación de las que forma parte Internet. Hay que hacer de este último un patrimonio abierto a todos y no el beneficio exclusivo de la delincuencia. (Unión Internacional de Telecomunicaciones, 2007, p. 96)

Así, la protección del ciberespacio por parte de una nación implica el suministro sistemático de información relevante sobre los riesgos existentes en el mismo, tanto a las empresas como a los ciudadanos (Agence Nationale de la Sécurité des Systèmes d'Information, 2011, p. 14). Este ejercicio de transparencia, siquiera en foros reservados, pero desde luego con frecuencia en foros abiertos que trascienden incluso a la academia o los especialistas, contribuye además a la creación de una *"cultura del ciber riesgo"* que permite una mayor concienciación pública. De forma similar se pronunció el Consejo económico y social de las Naciones Unidas en el año 2011[11] y recientemente la Unión Europea (European Union Agency for Network and Information Security, 2014).

Tal y como afirman Underwood & Koskinen (2012), el enfoque educativo de la ciberseguridad parte de la sensibilización a los alumnos en edad escolar de los riesgos y las consecuencias de sus prácticas en Internet, a la vez que toma en cuenta otros actores responsables como los padres, organismos especializados y el propio sector de las telecomunicaciones en general.

Dicho esto, nuestro análisis del componente educativo en las EC parte de la información recopilada por el Centro de Cooperación y Excelencia para la Ciberdefensa de la OTAN,[12] el cual lleva un registro de todas las EC publicadas hasta el momento, según la siguiente tabla:

Tabla 1.

País	Año
Rusia	2000
Estados Unidos de América	2003
Malasia	2006
Australia	2009
Canadá	2010
Estonia	2010
Mongolia	2010
Alemania	2011
Francia	2011
Holanda	2011
Corea del Sur	2011
Lituania	2011
Luxemburgo	2011
Nueva Zelanda	2011
Reino Unido	2011
República Checa	2011
Uganda	2011

11. Jornada especial sobre ciberseguridad y desarrollo del 9 de diciembre de 2011. Ver resumen: http://www.un.org/en/ecosoc/cybersecurity/summary.pdf

12. Establecido en el año 2008, el Centro es una organización militar internacional acreditada por OTAN que trata la educación, consultoría, investigación y desarrollo del campo de la ciberseguridad. Los países patrocinadores del Centro son: Estonia, Alemania, Hungría, Italia, León, Lituania, Holanda, Polonia, Eslovaquia, España y Estados Unidos de América. Para más información visitar: https://ccdcoe.org/3.html

Austria	2012
Bélgica	2012
Dinamarca	2012
Georgia	2012
Hungría	2012
Jordania	2012
Mauritania	2012
Noruega	2012
Sudáfrica	2012
Suiza	2012
Trinidad y Tobago	2012
Arabia Saudita	2013
Egipto	2013
Eslovaquia	2013
España	2013
Finlandia	2013
India	2013
Italia	2013
Japón	2013
Marruecos	2013
Montenegro	2013
Panamá	2013
Polonia	2013
Rumanía	2013
Singapur	2013
Turquía	2013
Zimbabue	2013
Azerbaiyán	2014
Emiratos Árabes Unidos	2014
Ghana	2014
Grenada	2014
Jamaica	2014
Kenia	2014
Letón	2014
Mauritius	2014
Pakistán	2014

Fuente: Elaboración propia. (NATO Cooperative Cyber Defence Centre of Excellence, 2015).

De los 53 países listados, destacamos a simple vista lo siguiente: (1) La mayoría de las estrategias fueron publicadas en el año 2013. (2) Rusia y Estados Unidos de América fueron los dos primeros países en publicar su estrategia. (3) La ausencia notable de potencias económicas iberoamericanas (México, Colombia, Chile y Brasil).

Luego de revisar cada una de las estrategias listadas, se puede afirmar que 31 países (señalados en verde en la tabla precedente) incorporan expresamente el componente educativo dentro de sus EC. A continuación se reseñarán las principales iniciativas que a nuestro criterio merecen ser estudiadas por aquellos países que aún no han redactado su propia EC.

Se comenzará viendo las directrices educativas dirigidas hacia el colectivo militar y/o administrativo.

Para Dinamarca, su EC promueve que su personal militar se forme en temas de ciberseguridad en instituciones no militares, ya que estas en principio facilitan el paso al mercado laboral civil, si así deseasen los individuos en el futuro (Denmark Government, 2012, p. 20). Esta directriz sirve de base para argumentar que las instituciones educativas privadas danesas tienen buenas titulaciones en la materia.

En cambio, Jordania busca promover la concienciación sobre ciberseguridad mediante el desarrollo de un programa nacional de concienciación y entrenamiento sobre ciberseguridad, que incluya además al personal administrativo y militar (Ministry of Information and Communications Technology, 2012, p. 6). Esta directriz contrasta con la danesa, dejando en evidencia a las instituciones educativas privadas, ya que se encarga al gobierno la tarea de desarrollar dicho programa.

Pasando al ámbito propiamente académico o universitario, la EC de Estados Unidos de América del año 2003 reconocía ya en aquel entonces el rol vital que juegan las instituciones de educación superior dentro de la promoción y debate del tema de ciberseguridad en cualquier nación (The White House, 2003, p. 40). Han pasado más de diez años

desde la redacción de este documento, con lo cual conviene analizar detenidamente la experiencia de este país, el cual es un referente en la materia de ciberseguridad y ciberdefensa a nivel mundial.

Actualmente, Estados Unidos de América cuenta con una plataforma llamada la National Initiative for Cybersecurity Education (NICE), la cual fue establecida en el año 2012 por el gobierno federal[13] y que como su propio nombre indica, busca promover el desarrollo de capital humano en el tema de ciberseguridad. Esta plataforma está coordinada por el Departamento de Comercio y enmarca todas sus acciones dentro de tres pilares estratégicos (NICE, s.f.):

> (1) Concienciación sobre ciberseguridad: liderado por el Department of Homeland Security (DHS), estas acciones buscan promover un uso responsable del internet entre la población en general mediante campañas publicitarias públicas.[14] (b) Educación formal sobre ciberseguridad: liderado por el Department of Education, DHS y el National Science Foundation. Estas acciones buscan incorporar programas de ciberseguridad en todos los niveles educativos incluyendo el preescolar.[15] (c) Personal especializado en ciberseguridad: liderado por el Department of Labor, Deparment of Defense, Office of Personnel Management y DHS. Estas acciones buscan el fomento y desarrollo de profesionales especializados en ciberseguridad y Ciberdefensa. (NICE, s.f.)[16]

Al analizar las iniciativas englobadas por NICE desde su creación, se evidencia un gran nivel de planificación, desarrollo y despliegue de recursos relacionados con la educación y la ciberseguridad a lo largo de los años que ningún otro país ha logrado hasta el momento. Esta experiencia es a nuestro entender una hoja de ruta que ha inspirado a todos los demás países con EC, debido a la gran variedad de iniciativas y proyectos desarrollados por Estados Unidos de América en el campo educativo.

Esta influencia es evidente, por ejemplo, en el caso del Reino Unido. En lo que se refiere a la promoción de expertos en ciberseguridad dentro del sector privado, el Gobierno del Reino Unido recomienda lo siguiente: (a) Fortalecer la oferta educativa a nivel de postgrado. (b) Diseñar una agenda de investigación multidisciplinaria. (c) Crear un instituto de investigación en ciberseguridad (National Security and Intelligence, 2011, p. 29).

La Office of Cyber Security & Information Assurance -OCSIA-[17]es el organismo británico que coordina todas estas iniciativas. Hasta el momento, se le puede acreditar en el campo de educación la creación de una asignatura a nivel de secundaria sobre ciberseguridad, así como una competencia interuniversitaria sobre ciberseguridad (CSC. s.f.).

En lo concerniente al público o la ciudadanía en general, destacamos el caso de Australia, en la cual una las siete prioridades estratégicas de su EC es la educación y empoderamiento de todos los ciudadanos australianos con la información, confianza y herramientas prácticas que necesitan para protegerse en el ciberespacio (Australian Government, 2009, p. 10). Para lograr estos fines, el gobierno australiano ha emprendido las siguientes acciones:

> (a) La creación de un portal de internet estatal único que proporcione información, consejos y alertas sobre ciberseguridad a los usuarios domésticos y las pymes (SSO, s.f.). (b) La incorporación de módulos educativos sobre ciberseguridad en los niveles de primaria y secundaria. (c) La celebración anual de la "Cyber Security Awareness Week" o semana de la concienciación sobre la ciberseguridad,

13. El plan estratégico de NICE se puede ver en http://csrc.nist.gov/nice/documents/nices-tratplan/nice-strategic-plan_sep2012.pdf
14. Un ejemplo de campaña publicitaria pública bajo este renglón es la campaña "Stop. Think.Connect". La misma ofrece, entre otros recursos, una guía interactiva para conocer las amenazas de ciberseguridad que afronta la población en general, desde la perspectiva de: adolescentes, padres, educadores, pymes, jóvenes profesionales e industria. Para más información ver http://www.stcguide.com/
15. Sobre este pilar destacamos los concursos organizados a nivel nacional sobre ciberseguridad y ciberdefensa. Estas competencias se desarrollan tanto en escuelas secundarias como en universidades, y consisten en ejercicios ofensivos y defensivos sobre ciberseguridad. Para más información visitar http://niccs.us-cert.gov/training/tc/search/cmp/new
16. De este pilar destacamos la "Cyberspace Workforce Strategy" redactada por el Departamento de Defensa a finales del año 2013. Este plan estratégico propone una serie de iniciativas relacionadas con el reclutamiento, entrenamiento y retención de mano de obra tanto del ámbito militar como del civil especializada en ciberseguridad y ciberdefensa. Para más información ver el plan estratégico completo en http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed%28final%29.pdf
17. Para más información visitar: https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance

> con la participación del empresariado, grupos de consumidores y organizaciones comunitarias. (Australian Government, 2009, p. 17)

De forma similar, el gobierno de Austria, mediante su objetivo estratégico número 13 de su EC busca la incorporación de la competencia de ciberseguridad en todos los niveles educativos, para lo cual sugieren las siguientes acciones:

> (a) Reforzar el grado de integración del tema de ciberseguridad en todos los niveles educativos, pasando a formar parte intrínseca del perfil de competencias digitales que todo estudiante debe poseer. (b) Incorporación de la ciberseguridad dentro del currículo formativo de profesores universitarios de forma que sea un requisito obligatorio para poder impartir docencia. (c) Aumentar la cantidad de expertos en ciberseguridad dentro del sector público a través de actividades formativas con instituciones nacionales e internacionales. (Bundesministerium Für Inneres, 2013, p. 15)

Hungría también busca integrar el tema de ciberseguridad en todos los niveles educativos, incluyendo entrenamientos especiales para empleados públicos (Government of Hungary, 2013, p. 5).En el caso de Eslovaquia, su EC solo busca incorporar el tema de ciberseguridad solamente en las escuelas secundarias (Slovak Republic, 2008, p. 16).

Por último, Japón, además de proponer programas de entrenamiento desde el nivel primaria, también incluye programas de entrenamiento para personas mayores o de la tercera edad (National center of Incident readiness and Strategy for Cybersecurity, 2013, p. 47).

Conclusiones

A la hora de diseñar e implementar acciones, proyectos e iniciativas educativas relacionadas con la ciberseguridad, sugerimos que las mismas estén enmarcadas dentro de una Estrategia de ciberseguridad nacional, tomando en cuenta las siguientes pautas: (1) Que abarque todos los niveles formativos: desde prescolar hasta universitario. (2) Que cuente con la participación de la academia tanto privada como pública. (3) Que tome en cuenta de la experiencia de otros países vecinos o de la misma región. (4) Que involucre directamente a los principales ministerios relacionados: educación, cultura, industria, etc.

Como hemos visto, la implementación, mantenimiento y mejora de una Estrategia de ciberseguridad nacional conlleva la consideración de una serie de factores transversales, dentro de las cuales destaca y predomina el factor educativo a todos los niveles sociales, desde los más especializados en los ámbitos militares y policiales a los más divulgativos para el público general.

También parece obvio que en el ámbito formativo, la coordinación entre el sector público y privado, entre los estamentos militares y de los cuerpos de seguridad de un lado y la sociedad civil a la que sirven de otro, es vital para el desarrollo e impartición de un currículo apropiado en todos los niveles educativos.

Los principales retos a los cuales se enfrentan los actores involucrados en las Estrategias de ciberseguridad nacionales son: (1) Asegurar la confianza y cooperación de otras naciones. (2) Integrar la educación en ciberseguridad en todos los niveles formativos. (3) Promover el desarrollo de expertos en ciberseguridad. (4) Asegurar la cooperación debida entre el estado, las empresas y los ciudadanos en general.

Para solventar estos retos recomendamos prestar especial atención a los siguientes objetivos: (a) Involucrar a las instituciones de educación superior e I+D, tanto públicas como privadas a la hora del diseño y redacción de la Estrategia de ciberseguridad. (b) Metas claras, específicas y de corto, medio y largo alcance dentro de la Estrategia. (c) Compartir el conocimiento y la información relativa a los objetivos de la Estrategia con la ciudadanía en general mediante acciones de difusión.

Referencias

Agence Nationale de la Sécurité des Systèmes d'Information. (2011). *Information systems defence and security. France's strategy*. Recuperado de: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf

Australian Government. (2009). *Cyber Security Strategy*. Recuperado de: http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf

Backstrom, A. & Henderson, I. (2012). Surgimiento de nuevas capacidades de combate: los avances tecnológicos contemporáneos y los desafíos jurídicos y técnicos que plantea el examen previsto en el artículo 36 del Protocolo I. *International Review of the Red Cross, 94*(886).

Baldwin, A. & Palfreyman, J. (2009). *Cyber defense: Understanding and combating the threat.* Nueva York: IBM Corporation.

Bundesministerium Für Inneres. (2013). *Austrian Cyber Security Strategy.* Vienna: Republik Österreich. Recuperado de: https://www.bka.gv.at/DocView.axd?CobId=50999

CCDCOE. (2015). Cyber Security Strategy Documents. *NATO Cooperative Cyber Defence Centre of Excellence*. Recuperado de https://ccdcoe.org/strategies-policies.html

CSC. (s.f.). Education and Development Overview. *Cyber Security Challenge UK*. Recuperado de http://cybersecuritychallenge.org.uk/education/education-and-development-overview/

Denmark Government. (2012). *Danish Defence Agreement 2013-2017*. Recuperado de: http://www.fmn.dk/eng/allabout/Documents/TheDanishDefenceAgrement2013-2017english-version.pdf

Droege, C. (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross, 94*(886), pp.533–578.

European Union Agency for Network and Information Security. (2012). *National Cyber Security Strategies*. Bruselas: European Network and Information Security Agency.

European Union Agency for Network and Information Security. (2014). *Public Private Partnerships in Network and Information Security Education*. Bruselas: European Network and Information Security Agency.

Government of Hungary. (2013). *Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary.* Recuperado de: http://www.nbf.hu/anyagok/Government%20Decision%20No%201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy%20of%20Hungary.docx

Klimburg, A. (Ed.). (2012). *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE Publication.

Lin, H. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross, 94*(886), 515–531.

Ministry of Information and Communications Technology. (2012). *National Information Assurance and Cyber Security Strategy -NIACSS-.* Recuperado de: http://nitc.gov.jo/PDF/NIACSS.pdf

Ministry of Security and Justice. (2011). *The National Cyber Security Strategy (NCSS)*. Recuperado de http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Netherlands_Cyber_Security_strategy.pdf

National center of Incident readiness and Strategy for Cybersecurity. (2013, June, 10). *Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace*. Recuperado de: http://www.nisc.go.jp/active/kihon/pdf/cybersecuritys-trategy-en.pdf

National Security and Intelligence. (2011). *The UK Cyber SecurityStrategy. Protecting and promoting the UK in a digital world*. Recuperado de: http://www.gov.uk/government/publications/cyber-security-strategy

NICCS. (s.f.). National Initiative For Cybersecurity Careers and Studies. *Department of Homeland Security*. Recuperado de http://niccs.us-cert.gov/

NICE. (s.f.). National Initiative For Cybersecurity Education (NICE). *National Initiative For Cybersecurity Education*. Recuperado de http://csrc.nist.gov/nice/index.htm

Rappert, B., Moyes, R., Crowe, A., & Nash, T. (2012). The roles of civil society in the development of standards around new weapons and other technologies of warfare. *International Review of the Red Cross, 94*(886), 765–785.

Shaw, L. (2014, December, 18). Sony's Costs From 'The Interview' Seen Near US$200 Million. *Bloomberg Business*. Recuperado de http://www.bloomberg.com/news/articles/2014-12-18/sony-s-costs-from-the-interview-seen-near-200-million

Slovak Republic. (2008). *National Strategy for Information Security in the Slovak Republic*. Recuperado de: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf

SSO. (s.f.). Stay Smart Online. *Australian Government Initiative*. Recuperado de http://www.staysmartonline.gov.au/

The White House. (2003, February). *The National Strategy to Secure Cyberspace*. Recuperado de: http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Underwood, J., & Koskinen, T. (2012). Ciberseguridad y educación. *Comisión Europea. Elearning Papers*, (28), 2–3.

Unión Internacional de Telecomunicaciones (2007). *Guía de ciberseguridad para los países en desarrollo*. Recuperado de: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf

Unión Internacional de Telecomunicaciones. (2010). Resolución 181: Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación. Conferencia de Plenipotenciarios. Recuperado de: http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

United States Government Accountability Office (2012). *Cyber Threats Facilitate Ability to Commit Economic Espionage. GAO-12-876T*. Recuperado de: www.gao.gov

White House. (s.f.). Cybersecurity Information Sharing Legislation. *US Government*. Recuperado de https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/information-sharing-legislation-section-by-section.pdf

ESCUELA SUPERIOR DE GUERRA

Fundada en 1909

Unión, Proyección y Liderazgo

ENCUENTRANOS EN:

Esdegue

issuu.com/esdeguecol

Esdeguecol

ESCUELA SUPERIOR DE GUERRA

Carrera 11 No. 102-50 Of. 327

Teléfono: 620 4066 · Ext. 21057

dirmaestrias@esdegue.mil.co

www.esdegue.edu.co