Elementos para una política de ciberseguridad efectiva

Antonio Fonfría | Universidad Complutense de Madrid.

Néstor Duch-Brown | Centro Común de Investigación (JRC, por sus siglas en inglés) de la Comisión Europea.

Tema

La política de ciberseguridad es diversa. Debe incluir necesariamente a agentes estatales, económicos y sociales, esclarecer cómo se ponderan los distintos objetivos entre sí e identificar claramente el papel que cumple el Estado en sus diversas funciones.

Resumen

La política de ciberseguridad se encuentra en un proceso de construcción que afecta al concepto, problemas y funciones a los que deben atender los Estados. La diversidad de actores, objetivos y prioridades complica la distribución de responsabilidades y condiciona el modelo de gobernanza aplicable. La evolución de los problemas de seguridad por solucionar modifica el papel del Estado, así como su capacidad para incluir todos los riesgos posibles dentro de su esfera de actuación. Este ARI analiza la evolución de las políticas de ciberseguridad, el papel del Estado y sus interacciones con los agentes económicos y sociales.

Análisis

"¿Qué es la ciberseguridad?". Lo que parece una pregunta sencilla es en realidad objeto de un gran debate tanto en foros nacionales como internacionales, políticos y académicos. En realidad, las actividades relacionadas con la ciberseguridad son notoriamente difíciles de acotar y esta falta de consenso permea no sólo en la posibilidad de establecer una definición generalmente aceptada del concepto, sino también en el gran debate —y reto político— alrededor de esta cuestión[1]. En este texto se intenta ofrecer un análisis de las razones que explican esta controversia con el objetivo de avanzar hacia una mejor comprensión de lo que es la ciberseguridad, con especial énfasis en el papel que posee el Estado en la definición de la política de ciberseguridad.

Una de las razones que explica la dificultad a la hora de definir la ciberseguridad es la continua evolución del concepto. No hace tanto tiempo, la ciberseguridad —o, más bien, sus conceptos predecesores, como la protección de infraestructuras críticas de información o la seguridad de la información— era una cuestión debatida principalmente

[1] Robert S. Dewar (2018), "National Cybersecurity and Cyberdefense Policy Snapshots", CSS (ETH Zurich), septiembre de 2018, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-eports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf.

en círculos especializados como un problema técnico o de gestión de riesgos. En los últimos años, se ha convertido en un problema de seguridad nacional —e internacional, dada la naturaleza de las redes de telecomunicaciones— abordado en los círculos más altos del Gobierno, en particular debido al marcado aumento de la actividad gubernamental en el ciberespacio por motivos estratégicos, que a su vez es un efecto colateral de las tensiones geopolíticas actuales[2]. Los ciberincidentes de alto nivel no sólo afectan a particulares o a empresas de forma individual, sino que también se consideran una amenaza para los Estados, las sociedades y las economías. Por consiguiente, los Estados están revisando sus propias capacidades ofensivas y defensivas y consolidando su planificación estratégica en relación con el uso del ciberespacio.

Sin embargo, la ciberseguridad no avanza sólo en las agendas políticas en todo el mundo. Paralelamente al avance de la digitalización, que se refleja en el aumento de la informatización y automatización de los procesos en las empresas y la sociedad, la ciberseguridad también se está expandiendo como ámbito de análisis y preocupación hacia esferas de algunas políticas que tradicionalmente no se encuentran en el acotado ámbito de influencia de la seguridad. Así, la ciberseguridad se está convirtiendo en un nuevo foco de atención para la educación y la formación al requerirse profesionales con las habilidades necesarias para desarrollar sistemas de ciberseguridad adecuados a las necesidades de diferentes usuarios. De la misma manera, aparece como una capacidad que promover en la cooperación al desarrollo, está vinculada a un nuevo tipo de diplomacia en la política exterior, es ya un elemento clave en la gestión de conflictos y, sin duda, se considera un sector empresarial importante o, de manera más general, la columna vertebral de la viabilidad económica en un mundo digitalizado[3]. La ciberseguridad es al mismo tiempo cada vez más importante, más diversa y más difundida.

La ciberseguridad y el papel del Estado

En primer lugar, *ciberseguridad* es un término relativamente nuevo, que aparece en la literatura especializada hacia el año 2000[4] y se desarrolla rápidamente desde entonces con un enfoque claramente multidisciplinar. Surge en el ámbito de las ciencias informáticas y se expande rápidamente hacia otras disciplinas técnicas primero y a la esfera social seguidamente. Dada su naturaleza, la ciberseguridad tiene significados distintos en diferentes ámbitos de análisis.

En origen, la motivación de ingenieros e informáticos para estudiar la ciberseguridad tenía el objetivo de aumentar la seguridad de los sistemas técnicos buscando un

[2] Marie Baezner y Patrice Robin (2017), "Cyber-conflict between the United States of America and Russia", CSS (ETH Zurich), junio de 2017, pp. 1-28, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-02.pdf.

[3] Dewar, Robert S. (2017), "The European Union and Cybersecurity: A Historiography of an Emerging Actor's Response to a Global Security Concern", en Maria O'Neill y Ken Swinton (eds.), *Challenges and Critiques of the EU Internal Security Strategy*, Cambridge Scholars Publishing, Newcastle upon Tyne, pp. 113-148.

[4] Rossouw von Solms y Johan van Niekerk (2013), "From information security to cyber security", *Computers & Security*, n.º 38, pp. 97-102, https://www.sciencedirect.com/science/article/pii/S0167404813000801.

compromiso entre los tres objetivos fundamentales de la seguridad informática: integridad, disponibilidad y confidencialidad de los recursos[5]. La "gobernanza de la ciberseguridad" es el concepto utilizado para alcanzar el objetivo, esencialmente un enfoque de gestión de riesgos basado en el seguimiento, la medición y el control continuos de los procesos relevantes. Aquí el concepto clave es la "regulación", que comprende diversas herramientas de gobernanza, como las normas industriales, las legislaciones nacionales o los acuerdos internacionales, con el objetivo primordial de generar confianza y mantener la estabilidad de las expectativas entre los distintos agentes.

Como es evidente, las aportaciones en materia de ciberseguridad desde un punto de vista técnico omiten, dada su naturaleza, el papel del Estado. Sin embargo, en el momento en que entran en juego cuestiones relacionadas con el intercambio de información y otras medidas organizativas, que suelen tratarse con más asiduidad en las ciencias sociales, el Estado se manifiesta de manera inmediata en su papel de regulador. Según la teoría de la gobernanza, ésta adquiere importancia cuando el poder político está muy fragmentado. La fragmentación del poder político puede producirse a través de la descentralización, cuando las tareas y la autoridad gubernamentales se delegan a entidades infra- o supranacionales, o bien a otros tipos de entidades (privatización)[6]. Esta fragmentación también puede tener lugar en el interior del propio Estado a través de una cada vez mayor separación funcional de la Administración[7]. La creciente división del trabajo, característica específica de las sociedades más avanzadas, difumina la separación tradicional entre el sector público y el privado y provoca una reasignación de recursos, tareas y responsabilidades. Así, muchas de las tareas que anteriormente realizaba el Estado son ahora gestionadas por empresas especializadas.

En este sentido, un enfoque de "gobernanza en red" supone que las sociedades modernas requieren nuevas formas de Administración Pública[8]. Aquí se parte de la hipótesis de que el Estado ya no puede limitarse a dar instrucciones y supervisar su aplicación, sino que también debe configurar el espacio de interacción, de tal manera que la cooperación funcione correctamente incluso sin una supervisión constante. La Administración Pública se convierte así en una actividad en la que la persuasión, la negociación y la confianza mutua son más importantes que el control y la reglamentación. En este contexto, los servicios públicos se prestan a través de un conjunto de redes independientes que se regulan y organizan de manera autónoma. El papel del Estado en este tipo de solución organizativa puede adoptar diversas formas; por ejemplo, como garante de la seguridad, legislador, regulador o socio en materia de seguridad.

[5] Anderson, Ross (2008), Security Engineering: A Guide to Building Dependable Distributed Systems, 2.ª ed., Wiley.

[6] Elke Krahmann (2003), "Conceptualizing Security Governance", *Cooperation and Conflict*, n.º 38, pp. 6-26.

[7] Mark Bevir y R. A. W. Rhodes (2001), "A Decentered Theory of Governance: Rational Choice, Institutionalism, and Interpretation", *Working Papers of the Institute of Governmental Studies*, n.º 10.

[8] Guy Peters y John Pierre (1998), "Governance Without Government? Rethinking Public Administration", *Journal of Public Administration Research and Theory*, n.º 18, pp. 223-243.

Por el contrario, desde la perspectiva de las relaciones internacionales, la visión del Estado es más sencilla. En este caso, los Estados se consideran unidades comparables y es el equilibrio de poder lo que los obliga a actuar de manera específica. La capacidad ciberofensiva de un Estado es un instrumento abstracto de poder que puede utilizarse con diversos fines, tanto en tiempos de paz como durante conflictos. Sin embargo, los Estados son también actores llamados a restablecer el control del uso indebido del ciberespacio mediante las normas internacionales, a menudo buscando lecciones aprendidas de anteriores problemas y soluciones en materia de seguridad. En su papel de garantes de la seguridad, los Estados actúan o bien maximizando el poder o la seguridad o bien minimizando las amenazas.

Evolución de la política de ciberseguridad

En la década de 1980, se consideraba que las emergentes amenazas cibernéticas afectaban principalmente a las redes gubernamentales, por lo que las preocupaciones en materia de ciberseguridad de la época se centraron en el espionaje cibernético[9]. Es a partir de la década de 1990 cuando se observa un cambio cualitativo en la percepción de las amenazas. Gradualmente, se estableció una conexión entre infraestructuras de información y las denominadas infraestructuras críticas, aquellas en las que un fallo o un deterioro sustancial podría tener consecuencias dramáticas para la sociedad. La implantación de las tecnologías de la información en estas infraestructuras es una tendencia que avanza rápidamente y que genera enormes riesgos de ciberseguridad. Basta recordar la cantidad de ciberataques recibidos por hospitales durante la pandemia del COVID-19 para hacerse una idea de los riesgos asociados.

En la primera década de este siglo se registran dos cambios importantes. El primero consiste en pasar de los escenarios teóricos apocalípticos a la realidad de la ciberagresión en situaciones de conflicto, con consecuencias en los ámbitos público y privado. Detrás de este importante cambio está la “normalización” de los ciberconflictos como un complemento constante a los conflictos políticos. El segundo de los cambios radica en prestar más atención a los ataques selectivos. Por un lado, se registra un aumento de los denominados *mega hacks* o grandes ataques con éxito a objetivos económicos o políticos destacados. Por otra parte, el debate político se traslada hacia las denominadas “amenazas avanzadas persistentes” (*advanced persistent threats*, APT) que son agentes con capacidad de utilizar los medios cibernéticos para alcanzar objetivos específicos y habitualmente asociados a Estados que les aportan dicha capacidad, al menos inicialmnte. Ambos fenómenos señalizan la profesionalización y creciente sofisticación de los ciberdelincuentes y los ciberataques.

Sin embargo, aunque en los últimos años se ha informado mucho en los medios de comunicación sobre operaciones cibernéticas orquestadas por el Estado, los ataques de alto nivel con un impacto considerable siguen siendo relativamente raros. En la mayoría de los casos, los medios cibernéticos se utilizaron principalmente para llevar a

[9] Debido a factores históricos, políticos, sociales y económicos, Estados Unidos ha liderado la revolución de la información en sus primeras fases. De la misma forma, ha estado a la vanguardia del debate sobre la ciberseguridad. Véase Michael Warner (2012), “Cybersecurity: A Pre-history”, *Intelligence and National Security* 27, n.º 5, pp. 781-799.

cabo acciones perturbadoras y de desestabilización del entorno político. Solo en raras ocasiones se han utilizado para la destrucción, debido, por un lado, a las dificultades para lograr efectos claramente controlables y, por otro, a las estrategias de contención por parte de los Estados. En cambio, la gran mayoría de los ciberincidentes a los que se enfrentan cotidianamente empresas y particulares no reciben la misma atención mediática.

La relativa normalidad de la vida cibernética cotidiana obliga a plantear la posibilidad de una catástrofe cibernética dentro del proceso político. Para que esto funcione, la probabilidad de ocurrencia de dicho acontecimiento se presenta como inminente basándose siempre en anécdotas y sucesos menores, como "cuasiaccidentes", para ilustrar "lo que podría haber sido". Siguiendo dicha lógica, se utilizan hipótesis pesimistas, casi apocalípticas, asociadas a un enorme daño esperado. Así, la principal amenaza ya no proviene del riesgo real de ocurrencia de una catástrofe, sino más bien la inacción, más concretamente en el ámbito político. Finalmente, pero no menos importante, la reacción lógica a este tipo de representación del peligro resulta en un consenso social acerca de que el Estado no está haciendo lo suficiente por la ciberseguridad. Pero ¿qué puede —y debe— hacer el Estado en materia de ciberseguridad?

Papel del Estado en la política de ciberseguridad

Históricamente, se observa una evolución en las funciones del Estado que coincide con tres fases de la política de ciberseguridad. En una primera función, el Estado aparece como propietario de redes o sistemas de información que pueden estar en peligro. En una segunda función, es el actor que debe resolver el problema desde el punto de vista de la política de seguridad. En tercer y último lugar, el Estado —o ciertas unidades individuales del Estado— aparece como causante del problema. Es importante destacar que esta evolución es aditiva: se asumen nuevas funciones mientras se mantienen las antiguas, lo que aumenta la complejidad del ámbito de la política de ciberseguridad. Esta mutación en los roles y en la orientación de la política de ciberseguridad la revela como una cuestión transversal, que requiere la cooperación de una amplia variedad de agentes que proceden no solo de diversas autoridades públicas, sino también de las empresas y la sociedad civil.

El Estado por sí solo no puede garantizar una ciberseguridad efectiva, sobre todo porque muchas redes cruciales están en manos privadas. La ciberseguridad es también, en gran medida, responsabilidad de todos y cada uno de los agentes involucrados en el ciberespacio, desde empresas hasta individuos. No solo la industria —incluidas las pequeñas y medianas empresas— se ve especialmente afectada por la ciberdelincuencia y el espionaje; muchas infraestructuras críticas también son de propiedad privada, por lo que el Estado no puede garantizar su protección frente a ciberataques, aunque algunas de ellas, debido a su particular importancia, puedan ser protegidas por el Estado para complementar la responsabilidad privada. Además, la amplia gama de contramedidas necesarias incluye muchos elementos que el Estado no puede diseñar o aplicar por sí solo.

Sin embargo, el Estado debe asegurar sus propias redes civiles y militares contra todas las formas de conflicto cibernético por medios técnicos y de otro tipo. En esta función, actúa como garante y protector de las instituciones estatales básicas de la Administración. El Estado tiene, además, las funciones de legislador y regulador. Por una parte, diseña la base jurídica necesaria para aclarar su función jerárquica frente a la sociedad y la economía. Lo hace, por ejemplo, en la lucha contra la ciberdelincuencia o en la regulación de infraestructuras críticas. Por otra parte, también establece el marco jurídico para regular la tensión entre ciudadanos y empresas. Esto ocurre, entre otros casos, con las normas de seguridad requeridas en las certificaciones de productos o en la legislación sobre responsabilidad de los fabricantes por los productos y servicios basados en componentes digitales. La forma y la medida en que se ejerce este papel varían y dependen de la relación históricamente desarrollada entre la esfera económica y el Estado.

Además de cumplir con su papel de regulador, en el ámbito de las infraestructuras críticas el Estado también desempeña el papel de socio. Muchos países occidentales están intentando ofrecer una mayor protección a través de las denominadas asociaciones público-privadas. La mayoría de ellas se basan en entornos en los que se observa una cooperación voluntaria entre la industria y el Estado, especialmente en el ámbito del intercambio de información. Las asociaciones se basan en la idea de que, aparte de una nacionalización completa o una arquitectura de seguridad totalmente privada de las infraestructuras críticas, las cuestiones de seguridad nacional en el ámbito de la ciberseguridad solo pueden abordarse conjuntamente.

La sensibilización del público en general sobre las cuestiones cibernéticas supone también un importante esfuerzo político. El Estado desempeña a menudo el papel de creador y divulgador de conocimientos, en el que quiere ser percibido como una fuente fiable de información. Su éxito depende de la relación de confianza que se haya desarrollado históricamente entre los diferentes grupos de la sociedad y las instituciones estatales, en algunos casos de formas muy diferentes. En esta función, el Estado actúa como garante de la seguridad y utiliza su posición de confianza para difundir una determinada representación de los peligros subyacentes en el ciberespacio.

Si bien la relación de confianza es un componente importante del papel del Estado como promotor de una mayor ciberseguridad, las actividades de inteligencia pueden representar una amenaza para ciertos colectivos, como muchos ciudadanos cuya información personal puede ser violada. Esta dimensión no es nueva, pero se acentúa especialmente por el rápido progreso técnico observado en los últimos diez años. A nivel nacional, este puede ser el caso, por ejemplo, de la defensa contra el terrorismo y el espionaje, pero también en la prevención del extremismo político violento. En algunas sociedades, una historia de uso indebido de estas competencias por interferencias injustificadas del Estado en los derechos civiles refuerza la percepción del Estado como un peligro. Además, el espionaje político y económico procedente de Estados extranjeros refuerza la percepción de los Estados como fuentes de peligro. En este

papel, la acción estatal se considera, por tanto, un inconveniente; el Estado se convierte en el origen del problema[10].

Estado, economía, sociedad y ciberseguridad

Solo la cooperación efectiva entre los Gobiernos, las empresas y la sociedad puede lograr un nivel satisfactorio de ciberseguridad. Sin embargo, algunos subgrupos de estos actores tienen a menudo intereses diferentes. Esto da lugar a tres espacios de interacción que deben ser tomados en cuenta si se pretende diseñar una política de ciberseguridad efectiva. Dónde se posiciona exactamente la política de ciberseguridad en estos ejes y hacia dónde va es el resultado de complejos procesos de negociación que dependen, en gran medida, de acontecimientos individuales y percepciones de riesgo relacionadas.

El primer espacio de interacción ocurre entre el Estado y la economía. Aquí es necesario formular una política para asegurar las infraestructuras críticas que absorba las consecuencias negativas asociadas a los procesos de liberalización, privatización y globalización sin mermar sus efectos positivos. En este ámbito, el Estado está preocupado por la dependencia de la acción económica y la consiguiente resiliencia de la sociedad. ¿Cómo puede crearse confianza entre las empresas y las Administraciones Públicas? ¿Dónde debe intervenir el Estado para evitar la acumulación de riesgos y los efectos de contagio que suponen una amenaza para la sociedad? La búsqueda de respuestas a estas preguntas tiene lugar en este espacio y es, sin duda, una parte relevante del proceso político en materia de ciberseguridad.

Un segundo ámbito es el que aparece entre el Estado y los ciudadanos. En este caso, el problema reside en encontrar un equilibrio eficiente entre una mayor seguridad y una mayor libertad en el espacio digital. Un aumento de las competencias policiales o de inteligencia suele entrar en conflicto con los derechos civiles; en concreto, el derecho fundamental a la autodeterminación informativa o al anonimato en internet. Cuando se debaten en profundidad las amenazas cibernéticas, las personas tienden a olvidar que, a pesar de una mayor atención y un llamamiento a favor de una mayor y mejor protección, la ciberseguridad es solo uno de los muchos riesgos que el Estado debe abordar. A diferencia de amenazas como el terrorismo, en las que la percepción política y social del impacto sirve para legitimar recortes en las libertades y derechos fundamentales, los daños causados por incidentes cibernéticos del pasado no son lo suficientemente cuantiosos o no han provocado perjuicios directos como para que se acepte la imposición de costes elevados de protección o el recorte de los derechos civiles.

El tercer espacio de interacción aparece en las relaciones entre ciudadanos y empresas, en el que es necesario establecer las condiciones para el desarrollo de un ecosistema de seguridad satisfactorio. ¿Cómo puede regularse el mercado, que también se enfrenta al problema de los cuasimonopolios, de manera que se logre un equilibrio óptimo entre seguridad y funcionalidad? ¿Cómo pueden crearse incentivos para aumentar las

[10] Ronald J. Deibert (2018), “Toward a Human-Centric Approach to Cybersecurity”, *Ethics & International Affairs*, vol. 32, n.º 4, pp. 411-424.

obligaciones de seguridad para los proveedores de servicios? ¿Cómo se puede sensibilizar a los usuarios para anteponer la seguridad a la funcionalidad? ¿Cómo pueden armonizarse las condiciones del marco jurídico (mundial) para las actividades en el ciberespacio de cara a contrarrestar el peligro de las lagunas legales, así como del recurso a soluciones baratas?

Lo que dan por sentado los agentes económicos y de la sociedad civil también se aplica a las funciones del Estado: asume una multitud de funciones. Por lo tanto, no es sorprendente que, en muchos asuntos de política de ciberseguridad, el Estado represente al mismo tiempo una amplia variedad de intereses. Por consiguiente, se forman alianzas temáticas entre diferentes departamentos del Estado con diferentes grupos de interés de la economía y la sociedad. Cada uno de estos grupos políticos representa una visión diferente del papel del Estado en la cuestión de la ciberseguridad. En las democracias, estos conflictos de funciones se tratan a nivel político y pueden abordarse sistemáticamente. Por ejemplo, si bien el Estado tiene interés, a efectos de un enjuiciamiento penal eficaz y unas capacidades de inteligencia modernas, en el uso de vulnerabilidades para la vigilancia, también lo tiene en el mayor uso posible de tecnologías seguras y su utilización por parte de las empresas y la sociedad. En algunos Estados, este conflicto de objetivos se gestiona políticamente en un proceso institucionalizado de gestión de la vulnerabilidad. Así, entre otras cosas, el interés público en las plataformas seguras contrasta con el interés público en la eficacia de la aplicación de la ley. El reconocimiento de la legitimidad de las múltiples funciones del Estado contribuye a estructurar esta consideración de manera significativa desde el punto de vista institucional y a reconocer que las decisiones en este ámbito adoptan una dimensión política intrínseca.

Conclusiones

El análisis aquí presentado muestra que la política de ciberseguridad es diversa y debe incluir necesariamente a agentes estatales, económicos y sociales. El reconocimiento de la diversidad de la acción gubernamental es una base sólida para el desarrollo de opciones estratégicas que pueden desembocar en una estrategia global. Una estrategia global para la política de ciberseguridad debe establecer relaciones claras sobre cómo se ponderan los distintos objetivos entre sí y debe identificar claramente el objetivo que cumple el Estado en sus diversas funciones.

Aunque los resultados parecen ser diferentes en los distintos países, los espacios de interacción en los que se desarrolla la política de ciberseguridad son los mismos. La política de ciberseguridad gira principalmente alrededor de la definición de las distintas funciones del Estado, así como del resto de los agentes, en la materia[11]. Cabe señalar que tales funciones, en un entorno tecnológico y político en rápida evolución, son siempre transitorias y deben estar sujetas al control político.

Si bien los elementos de la discusión política son similares en distintos países, la manifestación concreta de las diferentes funciones depende, por un lado, de la fuerza

[11] Florian J. Egloff (2018), “Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates”, tesis doctoral, Universidad de Oxford.

de los distintos grupos de interés y, por otro, de la evolución histórica de la distribución de funciones y relaciones de confianza entre los agentes. Los temas relevantes incluyen cuestiones sobre los límites de responsabilidad —es decir, dónde empieza y termina la responsabilidad del Estado y de los agentes económicos y sociales— y sobre la asunción concreta de esta responsabilidad —qué medios pueden utilizar los agentes para desempeñar su función—. Como hemos visto, las respuestas a estas preguntas son el resultado de procesos políticos multifacéticos de ciberseguridad. Como elemento estructurador, los debates políticos deben circunscribirse a tres espacios de interacción, lo que permite un análisis más sistemático de los conflictos políticos en el ámbito de la ciberseguridad.