Spies, lies, and algorithms. The history and future of American Intelligence.
Amy B. Zegart. Princeton: Princeton University Press, 2022, 405 pp.

Amy B. Zegart se licenció en Estudios de Asia Oriental con la máxima calificación en la Universidad de Harvard y obtuvo un máster y un doctorado en Ciencia Política en la Universidad de Stanford. En la actualidad es *Senior Fellow* en la Hoover Institution, donde dirige el programa National Security Affairs Fellows. También es *Senior Fellow* del Instituto Freeman Spogli de Estudios Internacionales, catedrática de Ciencia Política (por cortesía) en la Universidad de Stanford y colaboradora de *The Atlantic*. Está especializada en inteligencia estadounidense, tecnologías emergentes y seguridad nacional, gran estrategia y gestión de riesgos políticos globales. Formó parte del Consejo de Seguridad Nacional de la administración Clinton y fue asesora de política exterior de la campaña presidencial de Bush en 2000.

Las investigaciones de Zegart, que han recibido distintos premios, se iniciaron con una interesante obra sobre la influencia del diseño institucional en los orígenes y evolución organizativa de tres organismos clave para la seguridad nacional de EE. UU.: la Agencia Central de Inteligencia, la Junta de Jefes de Estado Mayor y el Consejo de Seguridad Nacional, *Flawed by design: The evolution of the CIA, JCS and NSC* (1999). En este trabajo desarrolla con ingenio perspicaz la indagación desde la perspectiva de la teoría de la organización y del institucionalismo de elección racional combinadas con las realidades de la política estadounidense, fundamentadas en copiosos materiales históricos. En este libro provocador y reflexivo, Zegart pone en tela de juicio la creencia convencional de que los organismos de seguridad nacional funcionan razonablemente bien para servir al interés nacional tal y como fueron diseñados. Utilizando un enfoque institucionalista novedoso, la autora se pregunta qué fuerzas configuraron el diseño inicial de la Agencia Central de Inteligencia (CIA), la Junta de Jefes de Estado Mayor (JCS) y el Consejo de Seguridad Nacional (NSC), de tal manera que se vieron perjudicadas desde su nacimiento. Irónicamente, descubre que gran parte de la culpa puede atribuirse a las características más apreciadas de la democracia estadounidense —elecciones frecuentes, separación de poderes, gobierno de la mayoría, fórmulas de compromiso político—, que limitan el poder presidencial y dan al Congreso pocos incentivos para crear un sistema eficaz de política exterior. Al mismo tiempo, los burócratas de los departamentos rivales tenían la experiencia, el poder de la permanencia y los

incentivos para obstaculizar la creación de competidores eficaces, y eso es exactamente lo que hicieron.

Las pruebas históricas sugieren que la mayoría de los actores políticos no tuvieron en cuenta las preocupaciones nacionales generales cuando forjaron la CIA, la JCS y el NSC a finales de la década de 1940. Aunque el presidente Truman pretendía establecer un sistema funcional de política exterior, se vio obstaculizado por burócratas civiles, legisladores y líderes militares con intereses propios. El NSC se creó por accidente, como subproducto de un compromiso político; la oposición de la Marina paralizó a la JCS desde el principio, y la CIA surgió sin la autoridad estatutaria para cumplir la función que se le había asignado gracias a que los departamentos de Marina, Guerra, Estado y Justicia, lucharon ferozmente para proteger sus propios aparatos de inteligencia.

No es de extrañar que las nuevas agencias de seguridad obtuvieran malos resultados mientras luchaban por superar su dañada evolución. Solo el NSC superó sus desventajas iniciales, ya que varios presidentes aprovecharon las lagunas de la Ley de Seguridad Nacional de 1947 para reinventar el personal del NSC. La JCS, por el contrario, permaneció estancada en su ineficaz diseño durante casi cuarenta años —es decir, durante toda la Guerra Fría—, y la rama de análisis fundamental de la CIA nunca se ha recuperado de sus orígenes. En resumen, la autora traza un cuadro sorprendente: los organismos con los que más cuentan los estadounidenses para protegerse de sus enemigos en el extranjero son incapaces de hacerlo, en gran medida por su propio diseño.

Zegart es autora también del principal estudio académico sobre los fallos de los servicios de inteligencia antes del 11-S: *Spying blind: The CIA, the FBI, and the origins of 9/11* (2007). En este imprescindible trabajo, Zegart ofrece el primer examen académico de los fallos de adaptación de las dos principales agencias de inteligencia que precedieron a los ataques terroristas del 11 de septiembre de 2001. Hasta entonces, esos fallos se habían atribuido en gran medida a errores individuales. Pero Zegart muestra cómo y por qué el propio sistema de inteligencia hizo vulnerables a los Estados Unidos. La autora argumenta que, tras el fin de la Guerra Fría, la CIA y el FBI no se adaptaron al incremento y a las nuevas variedades del terrorismo. Para ello, realiza un minucioso análisis de más de trescientas recomendaciones de reforma de los servicios de inteligencia y recorre la historia de los esfuerzos antiterroristas de la CIA y el FBI desde 1991 hasta 2001, basándose en documentos oficiales desclasificados y en entrevistas con más de setenta altos funcionarios gubernamentales.

Zegart revela que los dirigentes políticos eran muy conscientes del peligro terrorista emergente y de la necesidad urgente de reformar los servicios de inteligencia, pero no consiguieron que se realizasen los cambios que buscaban. La responsabilidad la tienen las mismas fuerzas que han obstaculizado la reforma de los servicios de inteligencia durante décadas: la resistencia dentro de las agencias; los intereses racionales de los políticos y los burócratas de carrera, y los aspectos fundamentales de la democracia estadounidense, como la estructura fragmentada del Gobierno federal. En última instancia, los fallos de adaptación organizativa condujeron a fallos de rendimiento. Zegart revela cómo las antiguas debilidades organizativas que no se afrontaron durante

la década de 1990 impidieron que la CIA y el FBI aprovecharan veintitrés oportunidades para desbaratar el complot del 11 de septiembre. Es un relato aleccionador de por qué dos de las agencias de inteligencia más importantes de Estados Unidos no se adaptaron a las nuevas amenazas después de la Guerra Fría y por qué es poco probable que se adapten en el futuro. Su lectura debería haber sido obligatoria para nuestros políticos y nuestros servicios de inteligencia y seguridad, debido a los ataques terroristas en nuestro suelo en Madrid (2004) y luego en Cataluña (2017).

Asimismo, Zegart es coautora, junto con Condoleezza Rice, de *Political risk: How businesses and organizations can anticipate global insecurity* (2018), basado en su popular curso conjunto en el MBA de Stanford. El mundo está cambiando rápidamente. El riesgo político —la probabilidad de que una acción política pueda perturbar significativamente al negocio de una empresa— está afectando a más compañías y de más formas distintas que nunca. Hace una generación, el riesgo político afectaba sobre todo a un puñado de industrias que trataban con Gobiernos en unos pocos mercados fronterizos. Hoy en día, el riesgo político proviene de una gama cada vez más amplia de actores, incluidos los usuarios de Twitter, los funcionarios locales, los activistas, los terroristas, los *hackers* y otros. Las mismas instituciones y leyes que se suponía que debían reducir la incertidumbre y el riesgo empresarial suelen tener el efecto contrario. En el mundo globalizado de hoy, no hay apuestas *seguras*. El libro de Rice y Zegart investiga y analiza este panorama en evolución, lo que las empresas pueden hacer para navegar por él y lo que todos nosotros podemos aprender sobre cómo entender y lidiar mejor con esta dinámica política global en rápido desarrollo. Basándose en las lecciones extraídas de los éxitos y fracasos de empresas de múltiples sectores, así como en ejemplos de operaciones de portaaeronaves, misiones de la NASA y otros lugares inusuales, este trabajo ofrece un marco de referencia conceptual inédito que puede aplicarse en cualquier organización, desde los *startups* hasta las empresas del IBEX.

Además, la profesora Zegart ha compilado con Herbert Lin, —codirectores del Programa de Política Cibernética de Stanford—, *Bytes, bombs, and spies: The strategic dimensions of offensive cyber operations* (2019). Las ciberoperaciones ofensivas se han convertido en elementos cada vez más importantes de la política de seguridad nacional de Estados Unidos. Desde el despliegue de Stuxnet para interrumpir las centrifugadoras iraníes hasta el posible uso de métodos cibernéticos contra los lanzamientos de misiles balísticos norcoreanos, la importancia de las capacidades ciberofensivas como instrumentos de poder nacional sigue creciendo. Sin embargo, el pensamiento conceptual va por detrás del desarrollo técnico de estas nuevas armas. ¿Cómo podrían utilizarse las operaciones ciberofensivas en la coerción o el conflicto? ¿Qué consideraciones estratégicas deberían guiar su desarrollo y empleo? ¿Qué capacidades de inteligencia son necesarias para que las ciberarmas sean eficaces? ¿Cómo funcionan la dinámica de la escalada y la disuasión en el ciberespacio? ¿Qué papel desempeña el sector privado? En este trabajo, destacados académicos y profesionales exploran estas y otras cuestiones vitales sobre los usos estratégicos de las ciberoperaciones ofensivas. Las contribuciones a este innovador volumen abordan las principales dimensiones técnicas, políticas, psicológicas y jurídicas del cambiante panorama estratégico.

Partiendo del bagaje descrito, en el libro objeto de esta recensión Zegart traza una panorámica fascinante sobre las realidades que afronta la inteligencia estadounidense de la que nosotros también tenemos mucho que aprender, como pone de manifiesto el reciente ciberespionaje a varios miembros del Gobierno español, cuya sorprendente filtración gubernamental ha servido para tratar de frenar la nueva campaña secesionista catalana sobre la materia con apoyo internacional, extremos sobre los que luego se añadirá un breve comentario.

El espionaje nunca ha sido más omnipresente ni menos comprendido. El mundo está anegado de películas, programas de televisión y novelas de espionaje, pero las universidades estadounidenses ofrecen más cursos sobre *rock and roll* que sobre la CIA y hay más expertos del Congreso en leche en polvo que en espionaje. En España la situación es todavía peor, si cabe. Esta crisis en la educación sobre los servicios de inteligencia distorsiona la opinión pública, alimenta las teorías conspirativas y perjudica la política de inteligencia y seguridad. En este libro, extraordinariamente documentado en noventa y seis páginas de notas, Zegart separa la realidad de la ficción al ofrecer un relato atractivo y esclarecedor del pasado, el presente y el futuro del espionaje estadounidense, que se enfrenta a una revolución impulsada por la tecnología digital.

Basándose en décadas de investigación y en cientos de entrevistas con funcionarios de los servicios de inteligencia, Zegart ofrece una historia del espionaje estadounidense, desde los espías de la guerra de la Independencia de George Washington hasta los satélites de espionaje de hoy en día. Examina cómo los espías ficticios están influyendo en los funcionarios reales; ofrece una visión general de los fundamentos de la inteligencia y de la vida dentro de las agencias de inteligencia de Estados Unidos; explica los sesgos cognitivos mortales que pueden inducir a error a los analistas, y explora las cuestiones controvertidas de los traidores, la acción encubierta y la supervisión del Congreso. Sobre todo, la autora describe cómo la tecnología está potenciando nuevos enemigos y oportunidades, y creando nuevos y poderosos actores, como los ciudadanos particulares que están rastreando con éxito las amenazas nucleares utilizando poco más que Google Earth. Y muestra por qué el ciberespacio es, en muchos sentidos, el último campo de batalla de capa y espada, donde los actores nefastos emplean el engaño, el subterfugio y la tecnología avanzada para el robo, el espionaje y la guerra de la información.

El capítulo introductorio describe el abanico de desafíos que afrontan los servicios de inteligencia en la era digital: los avances tecnológicos transforman las amenazas al generar nuevas incertidumbres y fortalecen a nuevos adversarios; la cantidad de datos *online* es tan abrumadora que es difícil de comprender y todavía más de darle sentido; el secreto habitual de las operaciones gubernamentales se pone en cuestión por las tecnologías emergentes que difuminan las antiguas fronteras de la geopolítica, pues la economía y la seguridad están ya estrechamente entrelazadas y desatan un mundo nuevo de información públicamente disponible o de fuentes abiertas.

El segundo capítulo examina la crisis en la educación en inteligencia y sus costes. La mayoría de los estadounidenses, incluidos los responsables políticos, tienen muy poca idea de cómo funcionan realmente las agencias de inteligencia de Estados Unidos. En su lugar, la ficción ha desempeñado un papel desmesurado. El entretenimiento con

temática de espionaje parece estar influyendo de forma significativa en las actitudes sobre los servicios de inteligencia. El dramático aumento del «entretenimiento de espionaje» implica prestar atención a cómo Hollywood ha alimentado las teorías conspirativas sobre un presunto «Estado profundo» y ha influido e influye en los responsables políticos y el público en general.

El tercer capítulo abarca el espionaje estadounidense desde la tinta invisible del siglo XVIII hasta los satélites de espionaje del siglo XXI. Puede parecer mucho tiempo, pero en comparación con el resto del mundo, la historia de la inteligencia estadounidense es bastante corta. Los espías de George Washington no aparecieron hasta dos mil años después de que el general chino Sun Tzu escribiera su tratado sobre el uso de la inteligencia en la guerra, *El arte de la guerra*. La vasta empresa de inteligencia actual surgió en gran medida después de la Segunda Guerra Mundial y refleja la evolución del papel del país en el mundo.

El cuarto capítulo trata de los fundamentos de la inteligencia. Examina lo que es la inteligencia, lo que no es y cómo funciona, con una panorámica sobre la caza de Osama bin Laden, que ha durado una década, y con reflexiones personales de funcionarios de inteligencia sobre su vida diaria, sus dilemas éticos y sus mejores y peores momentos. El quinto capítulo examina el análisis de inteligencia y por qué es tan difícil. Desde el ataque sorpresa de China en la guerra de Corea hasta los informes erróneos en torno a las armas de destrucción masiva de Irak, los fallos analíticos tienen causas comunes. La principal de ellas es lo que Zegart denomina los siete sesgos mortales o las trampas cognitivas que pueden llevar por el mal camino incluso a las mentes más inteligentes. También explora el mundo futuro de la inteligencia artificial, discutiendo qué tipos de análisis pueden hacer las máquinas mejor que los humanos y qué pueden hacer mejor los humanos que las máquinas.

El sexto capítulo aborda uno de los puntos más delicados para la Comunidad de Inteligencia: los traidores. ¿Qué motiva a los informantes de confianza a convertirse en traidores? ¿Cómo pueden los agentes de inteligencia reclutar espías en la era digital y cómo pueden identificar a posibles agentes dobles sin dejar de mantener la confianza necesaria para hacer su trabajo? El séptimo capítulo explora la acción encubierta, lo que el exdirector de la CIA, Leon Panetta, llamó una vez «un negocio difícil de decisiones angustiosas». Comienza en los desiertos de Yemen, donde un ciudadano estadounidense y terrorista infame llamado Anwar al-Awlaki fue asesinado en un ataque encubierto con drones sin juicio, juez ni jurado. Explora qué es exactamente la acción encubierta y por qué todos los presidentes la utilizan a pesar de que a menudo fracasa. Y recorre una de estas atormentadoras decisiones, examinando un hipotético dilema de acción encubierta desde diferentes perspectivas.

En el capítulo octavo examina el polémico mundo de la supervisión y el control del Congreso: cómo se ha desarrollado, por qué es importante, por qué rara vez funciona bien y qué nos depara el futuro. También se adentra en los debates sobre el programa de detenciones e interrogatorios de la CIA y el programa de escuchas telefónicas sin orden judicial de la NSA, dos de las controversias de supervisión más apasionadas de la historia de la inteligencia estadounidense.

El capítulo noveno se centra en la investigación nuclear en la era digital. Gracias a internet, a los satélites comerciales y a los análisis automatizados, la inteligencia nuclear ya no es solo cosa de los Gobiernos de las superpotencias. Se analiza el surgimiento de los nuevos detectives nucleares: personas y organizaciones ajenas a los Gobiernos que están transformando la forma de rastrear las actividades nucleares ilícitas. Este nuevo ecosistema informativo pone de manifiesto los drásticos cambios que se están produciendo hoy en día en el ámbito de la inteligencia, así como las oportunidades y los riesgos.

El capítulo décimo concluye con las ciberamenazas: qué son, cómo han evolucionado, qué significan para la inteligencia y los principales retos que plantean. En muchos sentidos, el ciberespacio es el último campo de batalla de capa y espada, donde los actores nefarios emplean el engaño, el subterfugio y la tecnología avanzada para el robo, el espionaje, la guerra de la información, etc. Las amenazas cibernéticas están hackeando tanto las máquinas como las mentes. Esto es solo el principio: la inteligencia artificial está creando vídeos, audios y fotografías ultra falsas *(deepfake)* tan reales que su inautenticidad puede ser imposible de detectar. Ningún conjunto de amenazas ha cambiado tan rápido y ha exigido tanto a la inteligencia. Para la Comunidad de Inteligencia de Estados Unidos y del resto del mundo occidental, la era digital está llena de complejidad y desafíos. Desde la captura de traidores y la realización de acciones encubiertas hasta la comprensión de las amenazas nucleares y la operación en el ciberespacio, el éxito requiere un replanteamiento fundamental sobre cómo asegurar la ventaja en un mundo radicalmente nuevo. Empieza por volver a lo básico y despolitizar de nuevo la inteligencia. Pero el éxito también incluye un cambio de misión que adopte la inteligencia basada en fuentes abiertas, desarrolle nuevas capacidades tanto para las actividades secretas como para el enfrentamiento abierto, y recompense a los funcionarios por hacer las cosas de forma diferente. Como se verá, adaptarse a esta era tecnológica supone un enorme cambio de paradigma. Pero es esencial.

Como es fácil colegir de este resumen apresurado, la importancia de las cuestiones abordadas en este libro tienen una tremenda actualidad, en especial en nuestro país. El valioso libro pionero de Díaz Fernández (2005) sobre nuestros servicios de inteligencia, como el resto de los estudios sobre asuntos de defensa y seguridad carece de la necesaria continuidad y de la suficiente atención en las universidades españolas. Acontecimientos recientes como el sorprendente reconocimiento de que los móviles institucionales del presidente del Gobierno y de algunos ministros habían sido hackeados y *gigabytes* de información sustraídos, se ha empleado como cortina de humo para encubrir una nueva sospechosa campaña del secesionismo catalán y así poder justificar el cese de la directora del Centro Nacional de Inteligencia. El profesor Olivas (2022a y 2022b) ha subrayado las graves dudas sobre la calidad y el rigor del informe sobre la supuesta vigilancia a dirigentes independentistas que continúan amenazando con la secesión de Cataluña.

El libro de Zegart es un relato fascinante y revelador del espionaje en la era digital, una lectura esencial para cualquiera que quiera comprender la realidad actual. El texto resultará de interés para el público culto en general y para distintas audiencias especializadas en la ciencia política y las relaciones internacionales. Debiera ser también de obligada lectura para políticos y periodistas de todos los partidos españoles.

Referencias

Díaz Fernández, Antonio. 2005. *Los servicios de inteligencia españoles desde la guerra civil hasta el 11-M. Historia de una transición*. Madrid: Alianza.

Lin, Herbert y Amy B. Zegart. 2018. *Bytes, Bombs, and Spies. The Strategic Dimensions of Offensive Cyber Operations*. Washington DC: The Brookings Institution. Disponible en: https://doi.org/10.1093/cybsec/tyx002.

Olivas, José Javier. 2022a. «"CatalanGate": escándalo útil, investigación teledirigida», *El Mundo*, 28-4-2022.

Olivas, José Javier. 2022b. «Methodological and ethical issues in Citizen Lab's spyware investigation in Catalonia». Disponible en: https://cutt.ly/sK33Qmx.

Rice, Condoleezza y Amy B. Zegart. 2018. *Political risk: how businesses and organizations can anticipate global insecurity*. Nueva York: Twelve.

Zegart, Amy B. 1999. *Flawed by Design. The Evolution of the CIA, JCS, and NSC*. Stanford: Stanford University Press. Disponible en: https://doi.org/10.1515/9780804764209.

Zegart, Amy B. 2007. *Spying Blind. The CIA, the FBI, and the Origins of 9/11*. Princeton: Princeton University Press. Disponible en: https://doi.org/10.1515/9781400830275.

JOSÉ A. OLMEDA
UNED