El desarrollo de la ciberguerra en el conflicto Palestino-Israelí



Clemente Olmedo. Estudiante de Relaciones Internacionales, Universidad Nacional de Rosario, Argentina.

Contacto: clemenolmedo10@gmail.com

Olmedo, C. (12 de junio, 2026). *El desarrollo de la ciberguerra en el conflicto Palestino-Israelí* [Artículo de opinión]. Centro de Estudios Estratégicos de Relaciones Internacionales. URL: https://www.ceeriglobal.org/el-desarrollo-de-la-ciberguerra-en-el-conflicto-palestino-israeli

Introducción

En la era de la interconectividad, la adopción de nuevas tecnologías representa un desafío transversal que impacta a todas las naciones dentro del sistema internacional. A medida que crece el número de personas y dispositivos conectados a internet, también se multiplican las vulnerabilidades cibernéticas que afectan diversos aspectos de la vida cotidiana. Frente a este escenario, los Estados han adoptado medidas orientadas a garantizar un ciberespacio más seguro y regulado. En este proceso, la lógica de la ciberseguridad ha transitado desde una perspectiva esencialmente defensiva hacia una concepción estratégica, en la que el control del ciberespacio se convierte también en instrumento de poder estatal. De esta manera, los actores estatales y no estatales han comenzado a emplear tecnologías digitales como herramientas ofensivas en el contexto de disputas y conflictos internacionales.

La región del MENA -Medio Oriente y Norte de África, por sus siglas en inglés- ha sido una de las regiones más afectadas a nivel mundial por ataques cibernéticos en el último año. En ese marco, la ciberseguridad se ha convertido en un elemento esencial para preservar la integridad, la confidencialidad y la disponibilidad de los datos y sistemas que operan en este vasto espacio virtual. En consecuencia, el ciberespacio en la región no queda exento de fracturas domésticas -como limitaciones institucionales y tensiones políticas internas-, desafíos gubernamentales y dilemas de seguridad, algunos de los cuales han perdurado durante muchos años.

En el conflicto palestino-israelí, las rivalidades históricas han sido potenciadas por la incorporación del ciberespacio como escenario de confrontación. Bajo la lupa del realismo ofensivo, Israel ha consolidado un ecosistema tecnológico que integra la ciberseguridad en su dimensión defensiva y ofensiva, materializando una ventaja estratégica que le permite proteger infraestructuras críticas, anticipar amenazas y neutralizar ataques en un contexto regional marcado por la volatilidad y la asimetría de poder. En este sentido, cada avance israelí en este terreno se traduce en un retroceso proporcional para las capacidades palestinas, configurando una dinámica de "suma cero". Esta supremacía digital no representa un mero complemento de la fuerza militar, sino el factor decisivo que ha inclinado el curso de las hostilidades en favor de Israel. En términos de Thomas Rid (2013), ello ha convertido al ciberespacio en un eje estructural del equilibrio de poder contemporáneo, donde la victoria y la seguridad en la región ya no se definen exclusivamente en el campo de batalla físico.

Desarrollo

La región fue escenario de lo que Wajsman (2022) identifica como la primera ciberarma utilizada a nivel global, abriendo un debate sobre el inicio formal de la "ciberguerra" en 2010 y consolidando al ciberespacio como un nuevo dominio de los conflictos armados que hasta hoy día perdura. Este ataque, conocido como *Stuxnet*, fue diseñado para sabotear el programa de enriquecimiento de uranio de Irán, cuya proyección de poder regional dependía en gran medida de su capacidad nuclear. Su empleo marcó el inicio de la redefinición de la percepción internacional sobre el uso de armas cibernéticas, al evidenciar su potencial para alterar equilibrios estratégicos sin recurrir a la fuerza convencional.

Este virus informático, desarrollado en conjunto por el Mossad -el servicio de inteligencia israelí- y la CIA, evidenció cómo la cibertecnología se incorporó de forma directa a la lógica del poder estatal en un conflicto internacional. Este código malicioso, caracterizado por ser un *rootkit,* se diseñó con el objetivo de atacar a los sistemas SCADA de las plantas nucleares iraníes. Su fin era interferir en los procesos industriales automatizados, y como resultado, se estima que aproximadamente el 20 % de las centrifugadoras de uranio en las instalaciones de Natanz y Bushehr fueron destruidas (Sánchez, 2012, pp. 129-130). Este ciberataque constituyó un verdadero punto de inflexión en la forma en que los Estados de la región comenzaron a percibir las estrategias derivadas del ámbito digital.

Otro caso emblemático de ello fue el ciberataque a Saudi Aramco en 2012 (Panetta, citado en Sanger & Shanker, 2012). Mediante un malware denominado *Shamoon*, Irán -según agencias de inteligencia de EE.UU.- logró borrar datos de aproximadamente 35.000 computadoras pertenecientes a la empresa petrolera, inutilizando sus redes internas y paralizando buena parte de sus operaciones administrativas. Este episodio expuso la vulnerabilidad de las infraestructuras críticas del Golfo y reveló la estrecha relación entre ciberseguridad y seguridad energética, impulsando a Arabia Saudita a fortalecer su política de ciberdefensa mediante la creación de nuevas agencias especializadas -como Aramco Digital- y la incorporación del ciberespacio como dimensión prioritaria de su estrategia nacional de Vision 2030 (Olech & Siekierka, 2021; PwC Middle East, 2024).

El posicionamiento de Israel como potencia cibernética en la región no ha sido un fenómeno espontáneo, sino el resultado de una estrategia de Estado sostenida a lo largo del tiempo. Desde principios de los años 2000, el gobierno israelí implementó una serie de programas de ciberdefensa coordinados, entre los que se destaca la National Cyber Initiative (2010), que dio origen a la Israel National Cyber Directorate (INCD), organismo encargado de articular los esfuerzos del sector militar, gubernamental y privado. Esta iniciativa se tradujo en una inversión significativa: solo en 2020, aproximadamente el 5 % del presupuesto total de defensa fue destinado a la dimensión cibernética, cifra que posiciona a Israel entre los países que más recursos asignan proporcionalmente a este ámbito. De este modo, se consolida una

doctrina nacional de ciberseguridad que trasciende la mera infraestructura técnica, integrándose como un componente estratégico del poder estatal.

El impacto de estas políticas ha sido doble: por un lado, consolidar a la Unidad 8200 como referente global en ciberoperaciones ofensivas y defensivas; por otro, fomentar un ecosistema de innovación tecnológica del cual surgieron empresas líderes como Check Point, NSO Group y CyberArk, reconocidas internacionalmente por su capacidad de exportar soluciones de seguridad digital (Cordey, 2019). Este entramado híbrido entre defensa nacional, innovación y sector privado ha permitido que Israel sea considerado no solo un actor clave en el plano regional, sino un referente ineludible en la configuración de la ciberseguridad a escala global, reforzando su poder tecnológico como extensión del poder estatal.

En contraste con el avanzado sistema cibernético israelí, tanto Hamas como Hezbollah han intentado desarrollar sus propias *ciberwings* como forma de resistencia y contraofensiva digital. En el caso de Hamas, desde mediados de la década de 2010 se han registrado intentos de infiltración en redes sociales y campañas de *phishing* dirigidas a soldados israelíes, así como la creación de aplicaciones falsas para recopilar información sensible (JISS, 2018). Hezbollah, por su parte, ha articulado células de ciberguerra con apoyo externo -principalmente a través de vínculos con Irán- desarrollando capacidades limitadas de espionaje y ataques de denegación de servicio -DDoS- (Freilich, 2024).

No obstante, estos esfuerzos reflejan más una búsqueda de compensar la disparidad que una capacidad real de equilibrar fuerzas: la diferencia tecnológica y de recursos sigue siendo abismal. En este marco, la contraofensiva cibernética de Hamas y Hezbollah no hace sino evidenciar la asimetría estructural de poder, donde la lógica de suma cero se traduce en que cada avance israelí amplía aún más esta brecha, reduciendo las posibilidades de sus adversarios de sostener un equilibrio en el ciberespacio.

Israel ha demostrado una notable capacidad de adaptación frente a las amenazas cibernéticas mediante la implementación de avanzadas herramientas tecnológicas. Este proceso no solo ha reforzado su capacidad defensiva nacional, sino que ha transformado la naturaleza del conflicto al trasladar parte de la confrontación con Palestina al dominio digital como forma de proyección del poder estatal. Como sostiene Nye (2010), el control del ciberespacio amplía las modalidades de influencia y reconfigura los equilibrios tradicionales de seguridad, difuminando las fronteras entre la guerra y la política.

Según Düz y Koçakoğlu (2025), tras la operación *Al-Aqsa Flood* del 7 de octubre de 2023, Israel incorporó sistemas basados en inteligencia artificial (IA) para la identificación de objetivos militares en Gaza. Tecnologías como *Lavender* y *The Gospel* fueron diseñadas por la Unidad 8200 y las IDF para procesar bases de datos con presuntos miembros de las facciones armadas de Hamás y la Yihad Islámica Palestina, a fin de generar blancos “precisos” para los bombardeos, como edificaciones e infraestructuras. A su vez, otra herramienta desarrollada con IA, *Habsora*, fue implementada con el propósito de acelerar la selección de objetivos mediante el análisis automatizado de información recolectada por drones, imágenes satelitales, redes sociales y comunicaciones interceptadas (Abraham, 2024). Sin embargo, el despliegue de estas tecnologías se inscribe en una doctrina militar que prioriza la eficiencia bélica y la rapidez operativa -con frecuencia por encima de la deliberación moral-, lo que exige una relectura crítica de la integración de la IA en escenarios de conflicto. Ello resulta especialmente relevante ante los dilemas éticos y los desafíos al Derecho Internacional Humanitario que plantea la automatización de funciones letales en la toma de decisiones (Scharre, 2018).

Israel, reconocido internacionalmente por su liderazgo en materia de ciberseguridad, ha consolidado una arquitectura de vigilancia de alta intensidad sobre la población palestina sustentada en herramientas de IA, tecnologías biométricas y sistemas de análisis masivo de datos, especialmente en Gaza y Cisjordania.

Informes de Naciones Unidas registran la presencia de 593 puestos de control y bloqueos viales en Cisjordania que restringen severamente la movilidad palestina. Asimismo, más de la mitad de los principales pasos que conectan Israel con Cisjordania y Gaza han pasado a manos de operadores privados desde el fin de la Segunda Intifada, un proceso asociado a la contratación de ex militares israelíes para tareas de seguridad (Loewenstein, 2023).

A partir de este entramado, las consecuencias de la vigilancia digital han profundizado mecanismos de control social y han abierto un escenario caracterizado por la creciente militarización tecnológica en contextos bélicos. La privatización de los puestos de control por parte de Israel, sumada a la expansión de sistemas autónomos y de monitoreo permanente, consolida lo que, en términos de Düz y Koçakoğlu (2025), constituye una "cárcel digital" sobre los territorios palestinos, donde la vigilancia se ejerce de manera sistemática e intrusiva. En este marco, la dimensión digital ha redefinido las formas contemporáneas de dominación política, en tanto la asimetría tecnológica opera como una herramienta que refuerza la subordinación de poblaciones vulnerables frente a Estados con mayores capacidades de innovación.

Conclusión

En síntesis, el dominio del ciberespacio se ha convertido en un instrumento decisivo para preservar o alterar el equilibrio de poder. Israel constituye un caso paradigmático: su avanzado ecosistema cibernético -resultado de la articulación entre Estado, industria tecnológica y esfera militar- le otorga una ventaja asimétrica en un sistema internacional marcado por la anarquía.

La incorporación de la IA al conflicto palestino-israelí evidencia cómo la innovación tecnológica no solo ha modernizado las dinámicas bélicas, sino que también ha transformado la naturaleza misma del conflicto hacia formas más automatizadas, predictivas y deshumanizantes. En este contexto, la IA redefine las estrategias de vigilancia, selección de objetivos y planificación militar, consolidando una lógica de confrontación cada vez más compleja y dependiente de capacidades digitales. De este modo, en un escenario global que avanza hacia la multipolaridad, la superioridad tecnológica emerge como un recurso central de poder y proyección estratégica.

No obstante, la hegemonía cibernética israelí trasciende el ámbito local. A nivel regional, redefine correlaciones de fuerza y acelera la competencia tecnológica con actores como Irán, Arabia Saudita y los Emiratos Árabes Unidos. A escala global, la exportación de sus modelos de vigilancia y capacidades cibernéticas contribuye a consolidar nuevos patrones de militarización digital y de control algorítmico. De esta forma, el caso israelí anticipa las tensiones que marcarán el futuro del poder en la era de la tecnología estratégica.

Abraham, Y. (3 de abril de 2024). *"Lavender": the AI machine directing Israel's bombing spree in Gaza.* +972 Magazine. https://www.972mag.com/lavender-ai-israeli-army-gaza/

Bergman, R., & Mazzetti, M. (28 de enero de 2022). *The battle for the world's most powerful cyberweapon.* The New York Times Magazine. https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

Buxbaum, J. (7 de septiembre de 2021). *Privatizing the occupation: How Israeli corporations came to police the Palestinians.* MintPress News. https://www.mintpressnews.com/privitizing-occupation-israel-corporation-police-palestinians/278411/

Cloudflare. (2024). *DDoS Threat Report Q1 2024.* Cloudflare, Inc.

https://www.cloudflare.com/learning/ddos/ddos-threat-report-q1-2024/

Cordey, S. (2019). *Trend analysis: The Israeli Unit 8200 – An OSINT-based study*. Center for Security Studies (CSS), ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf

Cunningham-Marsh, J. (2024). *MENA Cyber Summit 2025 Annual Report*. CS4CA MENA. https://mena.cs4ca.com/wp-content/uploads/MENA-Cyber-Summit-2025-Annual-Report.pdf

Düz, S., & Koçakoğlu, M. S. (2025). *Deadly algorithms: Destructive role of artificial intelligence in Gaza war* (SETA Publications No. 260). SETA Foundation for Political, Economic and Social Research. https://media.setav.org/en/file/2025/02/deadly-algorithms-destructive-role-of-artificial-intelligence-in-gaza-war.pdf

Freilich, C. (2024). *The Iranian Cyber Threat* (Memorandum 230). Institute for National Security Studies (INSS). https://www.inss.org.il/wp-content/uploads/2024/02/Memo230_IranianCyberThreat_ENG_digital.pdf

Dostri, O. (15 de octubre de 2018). *Hamas' Cyber Activity against Israel*. Jerusalem Institute for Strategy and Security. https://jiss.org.il/en/dostri-hamas-cyber-activity-against-israel/

Loewenstein, A. (2023). *The Palestine laboratory: How Israel exports the technology of occupation around the world*. Verso Books.

Nye, J. S. (2010). *Cyber power*. Harvard University, Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf

Olech, A., & Siekierka, K. (11 de agosto de 2021). Cybersecurity in Saudi Arabia. Institute of New Europe. https://ine.org.pl/en/cybersecurity-in-saudi-arabia/

PwC Middle East. (20 de diciembre de 2024). *Saudi Arabia emerging as global cybersecurity guardian*. PricewaterhouseCoopers. https://www.pwc.com/m1/en/media-centre/articles/saudi-arabia-emerging-as-global-cybersecurity-guardian.html

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies, 35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Rühle, M., & Urbelis, V. (2020). *Israel: Cybersecurity and cyber defense* (CSS Cyber Reports No. 9). Center for Security Studies (CSS), ETH Zürich. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf

Sánchez Medero G. . (2024). La ciberguerra: los casos de Stuxnet y Anonymous. *Derecom. Revista Internacional de Derecho de la Comunicación y de las Nuevas Tecnologías, 11*, 124-133. https://revistas.ucm.es/index.php/DERE/article/view/96207

Sanger, D. E., & Shanker, T. (2012, Octubre 11). Panetta warns of dire threat of cyberattack on U.S. *The New York Times*. https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Scharre, P. (2018). A*rmy of None: Autonomous Weapons and the Future of War*. W. W. Norton & Company.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Traynor, O. (6 de enero de 2025). *An overview of cyber attacks in the Middle East 2024*. CybelAngel. https://cybelangel.com/cyber-attacks-middle-east-2024/

Wajsman, G. (2022). Ciberguerra entre Israel e Irán: desde Stuxnet hasta los ciberataques actuales. *Anuario en Relaciones Internacionales del IRI; 2022*. Instituto de Relaciones Internacionales, Universidad Nacional de La Plata.