Guerra de quinta generación en la Cuarta Revolución Industrial

doi: 10.5281/zenodo.4654906

PIERO GAYOZZO https://orcid.org/0000-0002-5112-5431

Coordinador General de la Sociedad Secular Humanista del Perú (SSH). Fundador y Sub Director del Instituto de Estudios Transhumanistas (IET). Miembro de la Asociación Peruana de Comunicadores y Periodistas Científicos (APCIENCIA) y de la Asociación Peruana de Ateos - APERAT. Llevó estudios de ingeniería industrial en la Universidad de Lima. Miembro del Consejo del Fondo Editorial de la Sociedad Secular Humanista del Perú.

pgayozzo@ssh.org.pe @pgayozzo

La Cuarta Revolución Industrial promete grandes cambios sociales. Tal cual indica Klaus Schwab, esta revolución tecnológica alterará por completo los productos que elaboramos, cómo los elaboramos, cómo interactuamos y, sobre todo, quiénes somos. Como era de esperarse, aquel potencial caracterizado por la promesa de la automatización y la interconexión de los ecosistemas físicos con los digitales (Internet de las cosas, implantes neurales, prótesis inteligentes, etc.) no solo ofrecerían beneficios, sino que, consecuentemente, también supondrían peligros.

En 1989 la Gaceta del Cuerpo de Marines de los Estados Unidos publicó un artículo sobre las generaciones del quehacer bélico en la Historia Moderna (Lind et al., 1989). Este trabajo categorizaba la evolución de las tácticas empleadas en la guerra en 4 generaciones: la primera incluía aquellas propias de las guerras napoleónicas; la segunda, la guerra de trincheras de la Primera Guerra Mundial; la tercera, el blitzkrieg de la Segunda Guerra Mundial; y la cuarta generación de guerra, donde el escenario bélico presenciaría una difuminación entre lo civil y lo militar, el terrorismo moderno como una de sus expresiones.

Posteriormente, en la literatura se ha especulado sobre una quinta generación de guerra (5GW). Donald Reed (2008) la describe como un escenario en el que no siempre se conoce quién es el enemigo, de ahí que la catalogue como una guerra irrestricta. Esto quiere decir que en su desarrollo se emplean armas letales y no letales, militares y no militares, cualquier medio con que se pueda someter al adversario y obligarlo a aceptar la voluntad de una de las fuerzas en conflicto. En este nuevo contexto cuyo campo de batalla se torna omnipresente y en el que toda organización o persona puede ser un actor del conflicto, la victoria no es únicamente militar, ni se restringe a sus medios, sino que engloba las áreas económicas, científicas, sociales y políticas.

A esta idea Qureshi (2019) le agrega que la 5GW es también una batalla de las percepciones y de la información. Una nueva forma de conflicto rodeado de secretismo, una suerte de guerra cultural y moral librada desde el ciberespacio y los medios de comunicación en la cual se busca distorsionar la percepción social y la información disponible como arma para agitar masas, infiltrar una perspectiva mediante propaganda sin desencadenar violencia directa y reemplazar líderes políticos por unos títeres o simpatizantes del bloque nacional o internacional que desató las hostilidades.

En dicho escenario, las tácticas de combate han evolucionado y los adversarios pueden ser transnacionales o estados organizados, individuos o colectivos, ideologías o intereses de poder o económicos, la Cuarta Revolución Industrial hace su aparición.

En el presente artículo no recurriremos a describir un escenario 5GW Transhumano donde se compita por el mejoramiento humano o se especule sobre el quehacer bélico en una eventual singularidad tecnológica, como lo plantea McIntosh (2010), por ende, no será necesario el escepticismo frente al optimismo tecnológico sobre una 5GW que involucre adelantos en superinteligencia artificial o escenarios transhumanistas o arqueofuturistas como lo plantea Pankhurst (2014). Por el contrario, revisaremos brevemente la literatura disponible sobre la percepción que se posee de las tecnologías NBIC para la seguridad, así como la descripción de algunas propuestas aplicativas para la industria bélica.

Ciberguerra y los ecosistemas físico-digitales

(Guerra total)

La ciberguerra es la extensión del campo de batalla hacia el espacio virtual mediante operaciones sobre redes informáticas y tecnologías de la información. Dichas operaciones pueden ser divididas en tres rubros: ataques a las redes informáticas (destrucción del software o hardware), explotación de la red (obtención de data) y defensa de la red (Schreier, 2015). En la 4RI una ciberguerra podría librarse con novedades como el machine learning, el blockchain, la ciencia de datos e incluso la computación cuántica.

Uno de los ciberataques más sonados fue el ocurrido en Estonia el año 2007. El ataque fue incentivado en foros de Rusia y vulneró instituciones públicas y privadas del país báltico (Ottis, 2008). Producto de ello, Estonia emprendió modificaciones legales en materia de crímenes informáticos, creación de nuevas instituciones y de la Liga de la Ciberdefensa que reúne voluntarios en seguridad cibernética (Czosseck et al., 2011). El año 2015 la empresa Kyivoblenergo en Ucrania fue víctima de un ciberataque coordinado con el virus Blackenergy 3 a sus centrales eléctricas, evento que generó un apagón de casi 6 horas. En un entorno en el que los ecosistemas físicos-digitales estén interconectados ¿cuál sería el peligro?

Las infotecnologías aplicadas a la organización social traen consigo la emergencia de un nuevo modelo de ciudad: las Smart Cities. Estos espacios de convivencia se caracterizan por propiciar una interacción entre los ecosistemas físicos-digitales y una automatización de procesos para obtener un desarrollo sostenible, mayor seguridad y salud para sus habitantes (Lacinák & Ristvej, 2017). Debido a sus características y a estar conformada por un gran número de gadgets (Internet de las cosas), un ataque similar a los ocurridos en Estonia y Ucrania, podrían verse comprometidos no solo los usuarios a nivel personal, sino los suministros de servicios básicos, la información sensible de la localidad, empresas y procesos de seguridad y control. Algunas estrategias podrían ser el secuestro de datos (ransomware), hackeo de los sistemas de control de tránsito y, en términos generales, paralización de la producción y afectación de la convivencia en su interior.

Deep fakes (desestabilización casera)

Como se mencionó, se especula que el escenario de la 5WG no quede circunscrito al conflicto armado, sino que incluso las redes sociales servirían como plataformas de combate. Aquí podrían aprovecharse como nuevas armas informáticas los deepfakes. Los deepfakes son superposiciones, combinaciones y reemplazos de imágenes o videos usando aplicaciones de Inteligencia Artificial para crear videos falsos (humorísticos, pornográficos o políticos) que parecen auténticos. Estos videos falsificados pueden ser indistinguibles de videos originales y su amenaza radica en el potencial para minar la confianza en autoridades, generar crisis políticas, chantajear personajes públicos y difamar (Westerlund, 2019). Su uso para posicionar narrativas alternas o disidentes, nacionales o foráneas, podría propiciar tensiones innecesarias. Lo más peligroso es que las tecnologías necesarias para desarrollar deepfakes están al alcance de cualquiera y solo requieren de una computadora para su elaboración.

Bioterrorismo casero

Tras el 11 de septiembre, la estrategia del yihadismo individual fue evidenciada en los tutoriales para armar bombas caseras que Al Qaeda impartía en foros como Shumukh-al-Islam (Stenersen, 2013); por su parte, años más tarde el Estado Islámico ofreció tutoriales a sus seguidores de cómo convertir drones caseros en potenciales artefactos bélicos (Marín Delgado, 2018). Pese a que estos fueron usados en combate y no en atentados, en la residencia del autor del atentado del club Reina en Estambul se hallaron dos drones (Balkan, 2017).

Con dichos antecedentes y en vista de que atravesamos una época en que la democratización del conocimiento se ha popularizado y con ella nuevas tendencias han aparecido. ¿Qué podría hacer una organización similar en una sociedad en la que el biohacking no ha sido regulado?

Basado en la ética hacker, el colectivo de biohackers se auto-capacita en el conocimiento y uso casero de tecnologías para la experimentación biológica y modificación de elementos orgánicos (Coenen, 2017). Sus miembros no son necesariamente personas capacitadas en centros de educación superior, pueden serlo desde expertos reconocidos en la materia hasta simples curiosos. El peligro del biohacking reside en que las tecnologías que usa pueden ampliar la efectividad de agentes biológicos mediante ingeniería genética, ya sea para mantener su estructura, pero cambiar el componente activo por uno más perjudicial, modificar partículas para generar reacciones protectoras innecesarias en las personas infectadas, modificar el medio de transmisión del agente o potenciar virus con características de virus mortales

(Wikswo et al., 2014).

El riesgo de estos laboratorios caseros se traduce en el incremento de posibilidades de ataques bioterroristas, ya sea de naturaleza sanitaria o para afectar la biodiversidad de una región. De ahí que el 2016 James Clapper, Director de Inteligencia Nacional de Estados Unidos, agregara la ingeniería genética a la lista de armas de destrucción masiva (Regalado, 2016). ¿Cómo se podría evitar esta situación? Difícil respuesta. Quizás se deban emprender medidas de contacto directo con la comunidad biohacker como la ejecutada por el FBI en EEUU (Wolinsky, 2016).

Nanomateriales (Enfrentamientos bélicos directos)

En caso de un enfrentamiento bélico directo, la 4RI también tiene sus sorpresas. En vista de las peculiaridades que presentan los objetos a escala nanométrica, diversas estrategias aplicativas han sido propuestas. Desde hace algunos años, basados en la óptica de transformación se ha explorado la posibilidad de fabricar dispositivos de "invisibilidad" y camuflajes avanzados (cloak devices). De misma manera, en materia de defensa se investigan materiales auto-reparables, gracias a la adhesión de TiO2 o SiO, blindajes de tungsteno, Smart-Armours capaces de incluir la nanoelectrónica para ajustar desbalances de calor, monitoreo de signos vitales y ventilación en los trajes militares. Innovaciones similares ocurren en la industria aeroespacial, de telecomunicaciones, naval, de producción de bombas no-nucleares (Father of all bombs ruso) y otras (Sharon et al., 2019).

La 5GW en la Cuarta Revolución Industrial será el equivalente a una guerra de desestabilizaciones. Por ello, desde nuestra perspectiva se caracterizará por ser potencialmente:

- Difusa. Las diferencias entre actores y objetivos militares y civiles se borrarán aún más.
- Desestabilizadora social. Ataques informáticos con impacto en los ecosistemas físicos-digitales.
- Bioterrorista. Ataques sanitarios o a la biodiversidad.
- Auto-generada. El internet permitirá la auto-generación de armas autónomas o patógenos artesanales o caseros.
- Manipuladora. Orientación sistematizada de la opinión pública por redes sociales y narrativas falsas.
- Ubicua. Los "combatientes" pueden estar coordinados desde distintas partes del mundo en simultáneo.

Las tecnologías de la 4RI no solo afectarán el quehacer bélico, sino que podrían aumentar o mitigar lo que filósofos como Toby Ord o Nick Bostrom definen como riesgos existenciales. Queda claro que los peligros de las tecnologías del siglo XXI pueden no solo comprometer a un país o a una región, sino afectar directamente a todo el mundo. Para mitigarlos hará falta un diálogo más estrecho entre las autoridades y los activistas de comunidades independientes, así como un aumento significativo del poder y de la capacidad de decisión de las autoridades en la esfera internacional. Quizás optar por un gobierno global democrático y representativo capaz de hacer cumplir el derecho internacional y mantener la paz (Bunge, 2013) sea una alternativa que pronto tendremos que contemplar.

Como hemos visto, la Cuarta Revolución Industrial también transformará el concepto de guerra y pronto el campo de batalla será tanto nuestra vida física como la digital.

Referencias

Balkan, S. (2017). *Daesh's Drone Strategy. Technology and the rise of innovative terrorism.* SETA.

Bunge, M. (2013). *Filosofía Política. Solidaridad, cooperación y Democracia Integral.* Gedisa.

Coenen, C. (2017). Biohacking: New Do-It-Yourself Practices as Technoscientific Work between Freedom and Necessity. *Multidisciplinary Digital Publishing Institute Proceedings, 1*(3), 256. https://doi.org/10.3390/IS4SI-2017-04119

Czosseck, C., Ottis, R., & Talihärm, A. M. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. *International Journal of Cyber Warfare and Terrorism, 1*(1), 24-34. https://doi.org/10.4018/ijcwt.2011010103

Lacinák, M., & Ristvej, J. (2017). Smart City, Safety and Security. *Procedia Engineering, 192*, 522-527. https://doi.org/10.1016/j.proeng.2017.06.090

Lind, W. S., Nightengale, K., Schmitt, J., Sutton, J. W., & Wilson, I. (1989). The Changing Face of War: Into the Fourth Generation. En A. Karp, R. Karp, & T. Terrif (eds.), *Global Insurgency and the Future of armed conflict* (p. 8). Routledge. https://doi.org/10.4324/9780203089279

Marín, J. A. (29 de Enero de 2018). *El uso de drones comerciales como vectores terroristas.* Instituto Español de Estudios Estratégicos. http://www.ieee.es/Galerias/fichero/docs_marco/2018/DIEEEM03-2018_DronesComerciales-

VectoresTerroristas_JAMarinDelgado.pdf

McIntosh, D. (2010). *Transhuman Politics and Fifth Generation War*. Nimble Books.

Molist, M. (21 de enero de 2016). *Así es como un ciberataque deja toda una ciudad a oscuras.* El confidencial. https://www.elconfidencial.com/tecnologia/2016-01-21/amenazas-en-la-oscuridad-como-los-hackers-pueden-provocar-un-apagon-en-tu-ciudad_1138837/

Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Pankhurst, C. (23 de Mayo de 2014). *Posthuman prospects: Artificial Intelligence, Fifth Generation Warfare & Archeofuturism*. Counter-Currents. https://counter-currents.com/2014/05/posthuman-prospects/?__cf_chl_captcha_tk__=3acbe20097f9eb039d41cfc045a8169c653d34da-1607311778-0-AXwtDP2_Tym7Ctw7mEw4bpUbeVSsMnaCva5uZO1DIAh1zqLkjvskAOM19JB_2YAALqw1JoaPe6xX3NcvnFLitnCJfJbsDPNrBmeUfAwIfBcZEI8N9idaxC8TR

Qureshi, W. A. (2019). Fourth and Fifth Generation Warfare: Technology and Perceptions. *San Diego International Law Journal, 21*(1), 187-216. https://digital.sandiego.edu/ilj/vol21/iss1/7/

Reed, D. J. (2008). Beyond the War on Terror: Into the Fifth Generation of War and Conflict. *Studies in Conflict & Terrorism, 31*(8), 684-722. https://doi.org/10.1080/10576100802206533

Regalado, A. (9 de Febrero de 2016). *Top U.S. Intelligence Official calls gene editing a WMD threat*. MIT Technology Review. https://www.technologyreview.com/2016/02/09/71575/top-us-intelligence-official-calls-gene-editing-a-wmd-threat/

Schreier, F. (2015). *On Cyberwarfare*. DCAF Horizon. https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

Sharon, M., Silvestre, A., Rodriguez, L., Sharon, C., & Sifuentes, P. (2019). *Nanotechnology in the Defense Industry*. Scrivener Publishing.

Stenersen, A. (2013). 'Bomb-Making for Beginners': Inside al Al-Qaeda E-Learning Course. *Perspectives on Terrorism*, 25-37. http://www.jstor.com/stable/26296907

Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review, 9*(11), 39-52. https://doi.org/10.22215/timreview/1282

Wikswo, J., Hummel, S., & Quaranta, V. (2014). The Biohacker: A Threat to National Security. *Combating Terrorist Center Sentinel, 7*(1), 8-11. https://ctc.usma.edu/the-biohacker-a-threat-to-national-security/

Wolinsky, H. (2016). The FBI and biohackers: an unusual relationship. *EMBO Reports,* 793-796. https://doi.org/10.15252/embr.201642483

Cómo citar este artículo:

Gayozzo, P. (2021). Guerra de quinta generación en la Cuarta Revolución Industrial. *Futuro Hoy, 2*(1), 31-34. https://doi.org/10.5281/zenodo.4654906

Esta obra está bajo licencia internacional
Creative Commons 4.0 Reconocimiento 4.0.