# Análisis

## Daños colaterales: las posibles implicancias para Argentina de un conflicto convencional entre China y Estados Unidos

Mag. Esteban Crespo Kennedy

Un consenso que a esta altura debería ser evidente para la mayoría de la clase política, así como los miembros de la Comunidad de Defensa y Relaciones Internacionales, es que las crisis externas como la reciente pandemia y la guerra ruso-ucraniana han demostrado que no es necesario que el país se vea involucrado en un conflicto militar para sufrir daños económicos y sociales similares a los de una guerra.

Las recientes tensiones entre China y Estados Unidos por la isla de Taiwán parecen indicar un recalentamiento de la competencia estratégica entre ambos poderes. China no descarta usar su creciente poderío militar para una reunificación definitiva con Taiwán[1], mientras que Estados Unidos profundiza sus vínculos defensivos con la isla[2]. Si ambas potencias no logran articular una política de distensión efectiva, veremos una relación cada vez más dominada por el factor militar, donde los errores de cálculo podrían llevar a una escalada sin retorno en algún un futuro próximo[3] [4] [5].

Una guerra entre China y Estados Unidos será por intereses vitales, donde una China en ascenso buscará dominar la región del Pacifico, mientras que Estados Unidos y sus aliados usarán todos los recursos disponibles para impedirlo[6]. Esta podría convertirse en una guerra prolongada donde ambos tratarán de evitar una derrota que reconfigure la estructura de poder global[7]. Este conflicto impactaría de lleno en economía mundial debido a la centralidad que ocupa Asia en las cadenas de globales de producción industrial.

Este trabajo realizará un análisis preliminar con el fin de explorar posibles daños colaterales de operaciones militares como bloqueos navales, la ciberguerra y la guerra en el espacio para la Argentina, con el objetivo de proveer un disparador que alerte de la necesidad imperiosa de contemplar planes y estrategias orientados a mitigarlos en caso de que este conflicto se materialice.

### Bloqueos navales en el Mar del Sur de China

---

[1] Tiezzi, Shannon. "China's New White Paper Lays out Vision for Post 'Reunification' Taiwan". En: https://thediplomat.com/2022/08/chinas-new-white-paper-lays-out-vision-for-post-reunification-taiwan

[2] Zheng, Sarah: Soo Lindberg, Kari. "US Congress Forces Joe Biden Toward Risky Faceoff with China Over Taiwan". En: https://www.bloomberg.com/news/articles/2022-08-15/us-congress-forces-joe-biden-toward-risky-faceoff-with-china-over-taiwan

[3] Stavridis, James. "2022 look ahead: Arms race will dominate U.S. - China competition". En: https://asia.nikkei.com/Opinion/2022-look-ahead-Arms-race-will-dominate-U.S.-China-competition

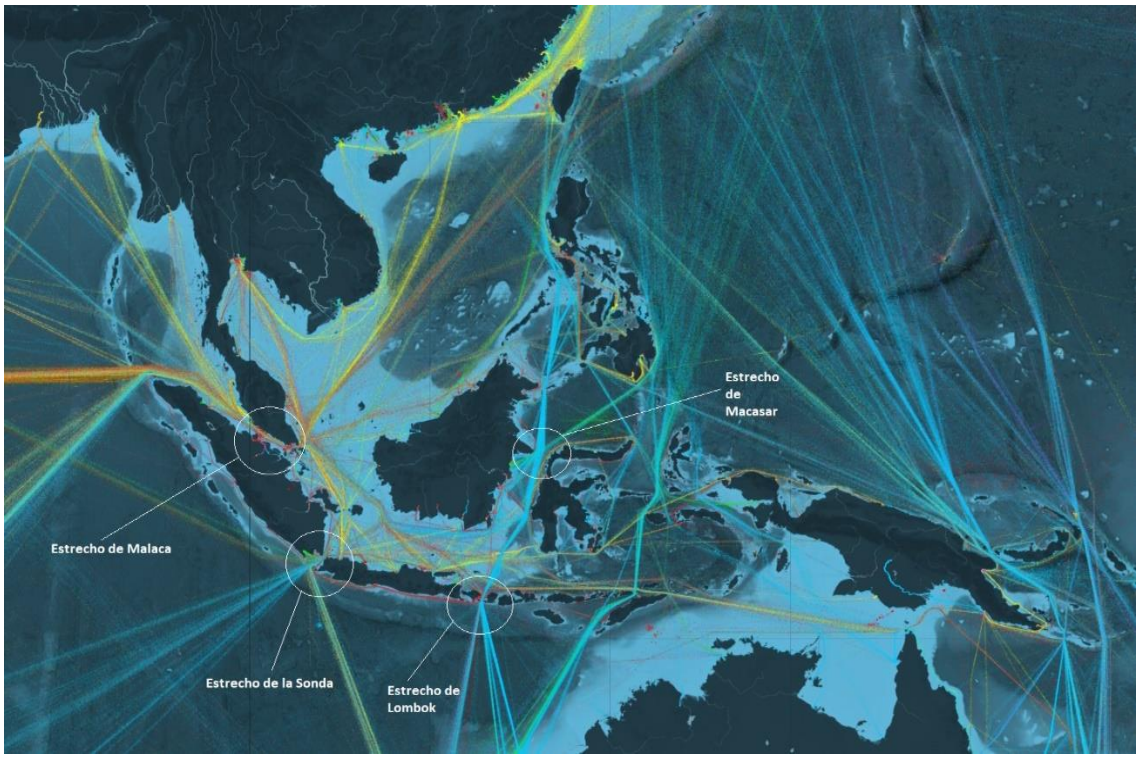
[4] Haenle, Paul; Bresnick, Sam. "Why U.S.-China Relations Are Locked in a Stalemate". En: https://carnegieendowment.org/2022/02/21/why-u.s.-china-relations-are-locked-in-stalemate-pub-86478

[5] Johnson, Jesse. "'Only a matter of time': Warnings of China-U.S. military miscalculation grow". En: https://www.japantimes.co.jp/news/2022/07/27/asia-pacific/china-us-military-miscalculation/

[6] Mearsheimer, John. "The tragedy of great power politics." New York: W. W. Norton & Company, 2014.

[7] Rovner, Joshua. "A Long War in the East: Doctrine, Diplomacy, and the Prospects for a Protracted Sino-American Conflict". En: https://www.tandfonline.com/doi/abs/10.1080/09592296.2017.1420535?cookieSet=1

Los bloqueos navales han sido aplicados de manera recurrente en conflictos entre grandes poderes,[8] y es una estrategia que ha sido sugerida con frecuencia en los círculos de planeamiento estratégico norteamericano para ser aplicada contra China en un conflicto militar. A lo largo de los años, esta estrategia, ha tomado diferentes nombres como: "*Off-Shore Control*[9]"; "*Stranglehold*[10]" y variantes similares[11] [12] [13].




Rutas Marítimas en el sudeste asiático[14] y sus principales puntos de estrangulamiento.

La premisa básica es que China no es un poder autárquico y depende en gran medida de sus exportaciones e importaciones para mantener su economía: alrededor del 20% de su PBI depende de las exportaciones[15] y es el mayor importador global de hidrocarburos[16], minerales industriales[17], alimentos[18], así como componentes críticos de tecnología para sus principales industrias de

[8] Mearsheimer, John. Op. Cit. P. 90
[9] Hammes, T. X. "Offshore Control: A Proposed Strategy". En: https://www.militarystrategymagazine.com/article/offshore-control-a-proposed-strategy
[10] Mirski, Sean. "Stranglehold: The Context, Conduct and Consequences of an American Naval Blockade of China". En: https://carnegieendowment.org/2013/02/12/stranglehold-context-conduct-and-consequences-of-american-naval-blockade-of-china-pub-51135
[11] Glab, Jason. "Blockading China: a guide". En: https://warontherocks.com/2013/10/blockading-china-a-guide/
[12] Wermeling, Ben. "Defeating Anti-Access/Area Denial in the West Pacific". En: https://thestrategybridge.org/the-bridge/2016/8/25/defeating-anti-access-area-denial
[13] Cornners, Matthew. "Blockade the First Island Chain". En: https://www.usni.org/magazines/proceedings/2019/june/blockade-first-island-chain
[14] https://www.shipmap.org/
[15] World Bank Data. En: https://data.worldbank.org/indicator/NE.EXP.GNFS.ZS?locations=CN
[16] Aizhu, Chen. "China's annual crude oil imports drop for first time in 20 years". En: https://www.reuters.com/markets/commodities/chinas-crude-oil-imports-post-first-annual-drop-20-years-2022-01-14/
[17] Roberts, Ivan; Saunders, Trent; Spence, Gareth; Cassidy, Natasha. "China's Evolving Demand for Commodities". En: https://www.rba.gov.au/publications/confs/2016/pdf/rba-conference-volume-2016-roberts-saunders-spence-cassidy.pdf
[18] Wang, Orange. "China food security: how's it going and why's it important?" En: https://www.scmp.com/economy/china-economy/article/3111623/china-food-security-hows-it-going-and-whys-it-important

circuitos integrados (chips), automotriz, salud y aeroespacial[19]. El 60% de su comercio internacional se realiza por vía marítima[20] y las rutas comerciales en la región poseen una serie de puntos de estrangulamiento naturales (Malaca, Sonda, Lombok y Macasar y otros pasos menores) entre Malasia, Indonesia, Filipinas[21], que pueden ser bloqueados en caso de un conflicto para forzar el colapso de la economía china.

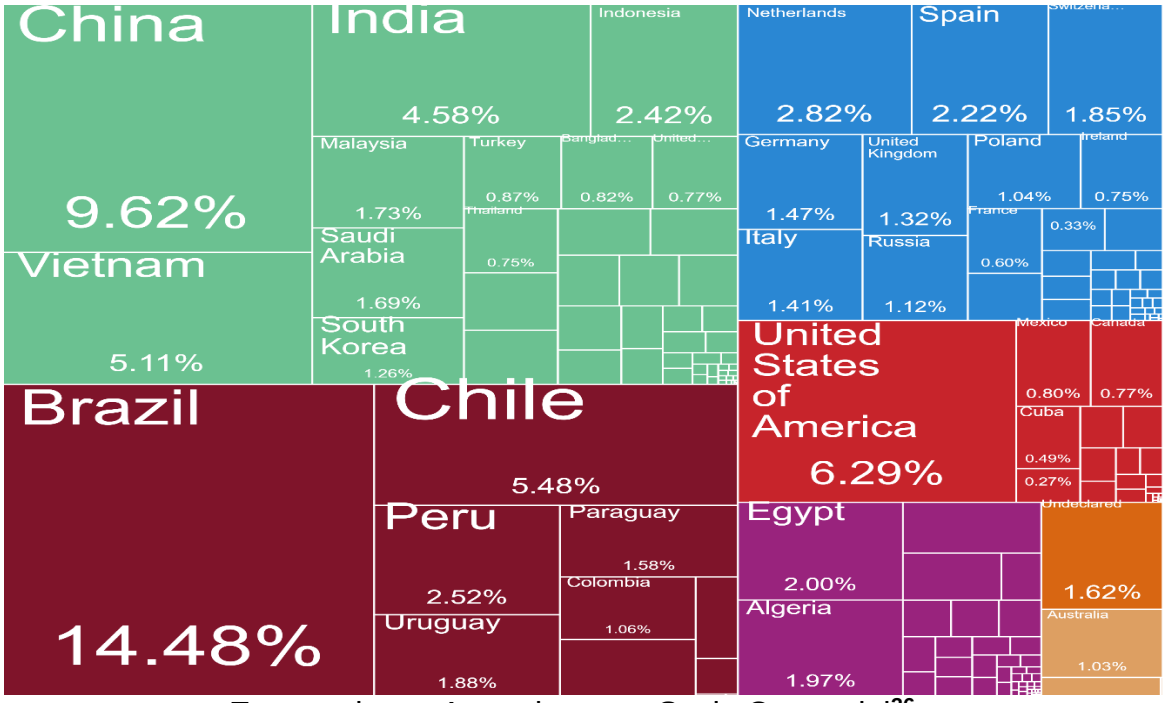
China denomina a esta estrategia de bloqueo como el "Dilema de Malaca" y a lo largo de los años ha buscado abrir nuevas rutas terrestres mediante la iniciativa del "*Belt and Road*". Sin embargo, aún faltarían años para que desarrollen rutas terrestres alternativas.[22] Asimismo, China podía aplicar una estrategia similar contra los aliados norteamericanos en la región[23] mediante el uso de sus submarinos, minado ofensivo u otras de sus capacidades de Anti-Acceso y Denegación de Área (A2/AD) para: "bloquear bases enemigas, puertos y rutas comerciales, destruyendo las capacidades de transporte marítimo del enemigo"[24], principalmente contra Taiwán[25] o Japón[26] que también es un gran importador de hidrocarburos[27]. Al mismo tiempo, ambos también se encuentran desarrollando planes orientados al bloqueo y uso de minado contra China[28] [29].

En este escenario, las operaciones de bloqueo y minado cruzado, embargos, sanciones comerciales[30], así como el aumento de los costos de transporte y los seguros[31], convertirán al Mar de Sur de China y posiblemente parte de los mares circundantes en una zona de exclusión para el tráfico marítimo civil. En este mar se encuentran las principales rutas comerciales para China, Japón, Corea del Sur, Taiwán y Hong Kong hacia los principales mercados globales, donde circula la mitad de la flota mundial y el 88% de los portacontenedores más grandes[32].

## El posible impacto económico de los bloqueos para Argentina

[19] Chiang, Min-Hua. "China More Dependent on U.S. and Our Technology Than You Think" En: https://www.heritage.org/asia/commentary/china-more-dependent-us-and-our-technology-you-think
[20] CSIS. "How Much Trade Transits the South China Sea?". En: https://chinapower.csis.org/much-trade-transits-south-china-sea/
[21] "China's Maritime Chocke Points". En: https://geopoliticalfutures.com/chinas-maritime-choke-points/
[22] Khan, Abdullah. "The Malacca Dilemma: A hindrance to Chinese Ambitions in the 21st Century". En: https://bpr.berkeley.edu/2019/08/26/the-malacca-dilemma-a-hindrance-to-chinese-ambitions-in-the-21st-century/
[23] "China drills reveal plans for Taiwan blockade: experts". En: https://www.france24.com/en/live-news/20220806-china-drills-reveal-plans-for-taiwan-blockade-experts
[24] Erickson, Andrew S.; Murray, William S.; Goldstein, Lyle J. "Chinese Mine Warfare: A PLA Navy 'Assassin's Mace' Capability". En: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1002&context=cmsi-red-books
[25] Kawakami, Yasuhiro." Mine Warfare in a Taiwan Contingency — Scenarios for Naval Mine Use and Its Impact on Japan". En: https://www.spf.org/iina/en/articles/kawakami_01.html
[26] Golstein, Lyle J. "China Thinks the United States Can't Handle Sea Mines". En: https://nationalinterest.org/blog/reboot/china-thinks-united-states-cant-handle-sea-mines-194845
[27] Hinkley, Dustin. "Japan Needs an Energy Security Strategy for the Taiwan Strait". En: https://thediplomat.com/2021/12/japan-needs-an-energy-security-strategy-for-the-taiwan-strait/
[28] Axe, David." Japan Has a Plan for Dismantling China's Submarine Fleet". En: https://www.forbes.com/sites/davidaxe/2020/06/22/japan-has-a-plan-for-dismantling-chinas-submarine-fleet/?sh=3891556c6d6c
[29] "Taiwan adds minelaying ships to defenses against China". En: https://www.defensenews.com/naval/2022/01/14/taiwan-adds-minelaying-to-defenses-against-china/
[30] "Taiwan says hopes world would sanction China if it invades". En: https://www.reuters.com/world/asia-pacific/taiwan-says-hopes-world-would-sanction-china-if-it-invades-2022-05-07/
[31] "Risk Insurers Shy Away from Taiwan Amid Tension with Beijing". En: https://www.wsj.com/articles/risk-insurers-shy-away-from-taiwan-amid-tension-with-beijing-11659973051
[32] Varley, Kevin. "Taiwan Tensions Raise Risks in One of Busiest Shipping Lanes". En: https://www.bloomberg.com/news/articles/2022-08-02/taiwan-tensions-raise-risks-in-one-of-busiest-shipping-lanes#xj4y7vzkg

Los efectos más inmediatos de una estrategia de bloqueo para la Argentina serían los financieros[33]. En los primeros días del inicio de las hostilidades, se vería un colapso de los mercados mundiales. China es nuestro mayor socio comercial[34] y la súbita afectación de la demanda China y de los otros países de la región generaría un exceso de oferta que empujaría una caída de las cotizaciones de los principales commodities de exportación de país. En esta misma situación se encontrarían nuestros principales socios que también dependen de los mercados de Asia para sus exportaciones[35], lo que generaría una fuerte contracción en sus economías y llevaría a una recesión global prolongada que podría afectar aún más las exportaciones nacionales.



Exportaciones Argentinas por Socio Comercial[36]

Por el lado de las importaciones, China, Taiwán, Hong Kong, Japón y Corea del Sur concentran más del 36% de toda la producción industrial del mundo[37], lo que incluye insumos críticos para salud, agricultura, la industria automotriz, el consumo masivo[38] y en especial los circuitos integrados.[39] Estos últimos juegan un rol crítico para las tecnologías de información y comunicaciones

[33] Frazier, Liz "The Coronavirus Crash Of 2020, And the Investing Lesson, It Taught Us". En: https://www.forbes.com/sites/lizfrazierpeck/2021/02/11/the-coronavirus-crash-of-2020-and-the-investing-lesson-it-taught-us/?sh=13320b0a46cf

[34] "Después de 18 meses, en enero China desplazó a Brasil como el principal socio comercial de Argentina". En: https://www.cronista.com/economia-politica/china-desplazo-a-brasil-como-el-principal-socio-comercial-de-argentina-en-el-primer-mes-del-ano/

[35] Kemp, John. "Column: China and the world economy's shifting centre of gravity". En: https://www.reuters.com/article/uk-china-economy-kemp-idUKKBN20S26Xhttps://www.reuters.com/article/uk-china-economy-kemp-idUKKBN20S26X

[36] Atlas of Economic Complexity: https://atlas.cid.harvard.edu/explore?country=8&product=undefined&year=2020&productClass=HS&target=Partner&partner=undefined&startYear=1995

[37] West, Drallel M. "Global manufacturing scorecard: How the US compares to 18 other nations". En: https://www.brookings.edu/research/global-manufacturing-scorecard-how-the-us-compares-to-18-other-nations

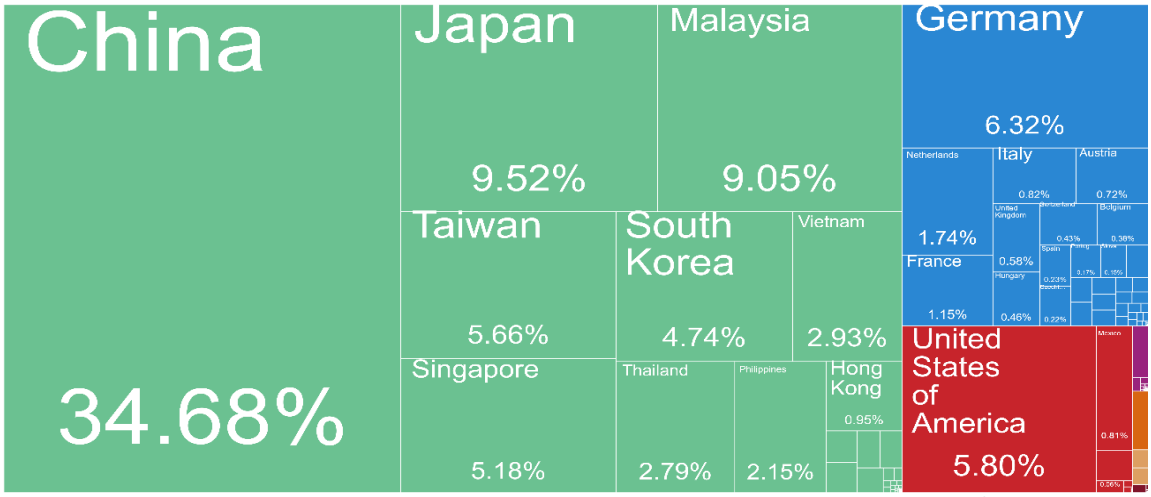
[38] Liuima, Justinas. "Supply Chain Sensitivity Index: Which Manufacturing Industries are Most Vulnerable to Disruption?" En: https://www.euromonitor.com/article/supply-chain-sensitivity-index-which-manufacturing-industries-are-most-vulnerable-to-disruption

[39] https://oec.world/en/profile/world/wld

(computadoras, celulares, tabletas, sensores, equipos de telecomunicaciones), así como otros miles de componentes electrónicos que son insumos para las principales industrias globales[40]. Una disrupción podría afectar seriamente a la industria nacional argentina, ya que el grueso de sus importaciones son bienes de capital e intermedios que abastecen la producción local[41].

La escasez de estos bienes impulsará un aumento de la inflación global, y también habría que considerar otros factores como cuáles serían las medidas que Estados Unidos tomaría para financiar la guerra, así como su impacto en el valor del dólar y la tasa de interés del tesoro americano.

La caída de los mercados financieros y las exportaciones de la Argentina, al igual que la de muchos países en condiciones similares, podría derivar en restricciones crediticias, salida de capitales, paralización de inversiones y una severa restricción externa de divisas que empujaría a una devaluación y afectaría los pagos de deuda; mientras que la imposibilidad de importar insumos críticos paralizaría las líneas de producción locales, lo que llevaría a una profunda depresión económica, una disparada en los niveles de pobreza y el desempleo. En su conjunto, el país podría enfrentarse a su mayor crisis en la historia.



Principales exportadores de circuitos integrados en 2020.[42]

**La Ciberguerra y la Guerra Espacial como posibles factores adicionales de daño con impacto nacional**

La segunda categoría de los efectos colaterales tiene que ver con posibles daños para la Argentina ocasionados por la ciberguerra y guerra en el espacio, que se han vuelto una parte integral de las doctrinas militares de China[43] y Estados Unidos[44]. Ambos países han demostrado extensas capacidades, desarrollando

[40] HIS Markit. "The role of East and Southeast Asia in the Global Value Chain in Electronics". En: https://ihsmarkit.com/research-analysis/the-role-of-east-and-southeast-asia-in-the-global-value-chain-.html
[41] CIRA. "Nuevo informe exclusivo de la CIRA: "las importaciones abastecen la producción". En: https://www.cira.org.ar/es/ejes-estrategicos/nuevo-informe-exclusivo-de-la-cira-las-importaciones-abastecen-la-produccion/
[42]https://atlas.cid.harvard.edu/explore?country=undefined&product=1744&year=2020&productClass=HS&target=Product&partner=undefined&startYear=1995
[43] "China's military strategy". En: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power
[44] "Posture statement of gen. Paul m. Nakasone, commander, U.S. cyber command before the 117th congress". En: https://www.cybercom.mil/media/news/article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-command-before-the/

organizaciones, procedimientos y tecnologías que les permiten ejecutar operaciones ofensivas dirigidas a las infraestructuras críticas de un adversario.

## La destrucción de infraestructura crítica como objetivo de las potencias en pugna

En años recientes se ha observado un uso más frecuente y disruptivo de los ciberataques: Estados Unidos habría realizado operaciones de reconocimiento contra las redes de distribución eléctrica y otros sistemas de infraestructura crítica en Rusia con el objetivo de inhabilitarlas en caso de un conflicto directo[45]. Planes similares habrían sido desarrollados contra Irán para atacar sus defensas aéreas, sistemas de comunicaciones, parte de sus redes de distribución eléctrica y centrales nucleares en caso de que no se lograra a un acuerdo sobre su programa nuclear[46]. Del mismo modo, China ha sido acusada de realizar ciberataques a gasoductos y oleoductos en Estados Unidos[47], intentar sabotear la generación y distribución eléctrica en la región de Ladakh en India[48], así como otros sistemas de infraestructura critica a lo largo de Asia[49].

Los ejemplos de la historia reciente sugieren que el alcance y potencial de daños podría derivar en serios riesgos para terceros. Stuxnet es el caso que muestra que un ataque a sistemas de control industrial, que son los encargados de mantener el funcionamiento de la infraestructura crítica, puede propagarse más allá de sus objetivos operacionales originales. Este malware tenía como objetivo sabotear los sistemas de control de las centrifugas de enriquecimiento de uranio en la planta iraní de Natanz.[50] Si bien se tomaron medidas para limitar su accionar a la configuración especifica de los sistemas de la planta, Stuxnet terminó escapando e infectando indiscriminadamente a miles de usuarios en 115 países[51].

Otro de los ejemplos está relacionado a los ataques a las redes de comunicaciones: hay indicios de que la Agencia Nacional de Seguridad (*NSA*) norteamericana enfoca sus esfuerzos en infiltrar los ruteadores y switches troncales, que son la columna vertebral de las redes que forman parte de internet,[52] y de ser necesario puede atacarlos para afectar el funcionamiento de "todo lo que sea importante para mantener a una sociedad funcionando: energía,

[45]Sanger, David E; Perlroth, Nicole. "U.S. Escalates Online Attacks on Russia's Power Grid". En: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

[46] Sanger, David E; Mazzetti, Mark. "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict". En: https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html

[47] CISA. "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013". En: https://www.cisa.gov/uscert/ncas/alerts/aa21-201a

[48] The Economic Times. "India has strong defence against cyber attacks: Power minister R K Singh". En: https://energy.economictimes.indiatimes.com/news/power/india-has-strong-defence-against-cyber-attacks-power-minister-r-k-singh/90711767

[49] Kovacs, Eduard. "China-Linked Cyberespionage Operation Suggests Interest in SCADA Systems". En: https://www.securityweek.com/china-linked-cyberespionage-operation-suggests-interest-scada-systems

[50] Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran". En: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[51] Paganini, Pierluigi. "An opportunity to reflect on Stuxnet and cyberweapons". En: https://resources.infosecinstitute.com/topic/the-zero-days-documentary/

[52] Zetter, Kim. "NSA Laughs at PCs, Prefers Hacking Routers and Switches". En: https://www.wired.com/2013/09/nsa-router-hacking

comunicaciones y transporte"[53]. En 2012, la NSA, en una fallida operación de inteligencia, afectó al 92% de los ruteadores de la red troncal de Siria mediante un ataque al Punto de Intercambio de Internet o *Internet Exchange Point* (IXP) de Damasco[54], lo que dejó al país sin internet durante varios días[55]. La NSA también habría logrado infiltrar a los fabricantes chinos de equipos de comunicaciones como Huawei, para obtener información sobre cómo explotar sus ruteadores y switches para operaciones de espionaje o ciber-ofensivas[56].

El tercer ejemplo involucra al uso de malwares como WannaCry, que afectó a 150 países y causó daños por 4.000 millones de dólares y Notpetya, atribuido a grupos afiliados al gobierno ruso, cuyo objetivo era realizar ciberataques a gran escala a la infraestructura crítica de Ucrania. Este ataque afectó a bancos, empresas, distribuidoras de energía eléctrica, transportes y aeropuertos, causando daños por más de 10.000 millones de dólares y dejando a más de 250.000 usuarios sin electricidad. Notpetya se expandió por 64 países[57], golpeando a su paso a grandes corporaciones como Maersk, la mayor naviera del mundo, paralizando sus operaciones globales en 86 puertos y al total de su flota[58].

Estos Malwares explotaban una vulnerabilidad llamada "Eternalblue", que fue parte de un conjunto herramientas para explotar vulnerabilidades (*exploits),* desarrollado por la NSA y que fueron expuestas en una brecha de seguridad en 2017[59]. Dentro de este paquete también se encontraban las instrucciones detalladas para hackear la infraestructura de servidores de la Sociedad para las Comunicaciones Interbancarias y Financieras Mundiales (SWIFT), que es uno de los pilares del sistema financiero global[60]. Lo que indicaría que los incidentes conocidos son sólo la punta del iceberg en lo que se refiere a la capacidad de atacar a sistemas que juegan un rol clave en el sostenimiento de las funciones diarias de una sociedad.

China tendría la capacidad para realizar operaciones similares. En años recientes Estados Unidos ha acusado a actores afiliados al gobierno chino de

[53] Der Spiegel. "NSA Preps America for Future Battle". En: https://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html
[54] Red, John. "Syrian Internet cutoff may be precursor to Assad offensive". En: https://foreignpolicy.com/2012/11/29/syrian-internet-cutoff-may-be-precursor-to-assad-offensive/
[55] Ackeman, Spencer. "Snowden: NSA accidentally caused Syria's internet blackout in 2012". En: https://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war
[56] Sanger, David E. "N.S.A. Breached Chinese Servers Seen as Security Threat". En: https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html
[57] Microsoft Defender Security Research Team. "New ransomware, old techniques: Petya adds worm capabilities". En: https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/?source=mmpc
[58] Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History". En: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[59] Gooding, Dan. "NSA-leaking Shadow Brokers just dumped its most damaging release yet" En: https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet
[60] "Hacking Group Claims N.S.A. Infiltrated Mideast Banking System". En: https://www.nytimes.com/2017/04/15/us/shadow-brokers-nsa-hack-middle-east.html

realizar ataques contra los gigantes tecnológicos como Google[61]y Microsoft[62]. La *Cybersecurity and Infrastructure Security Agency* (CISA) norteamericana los ha señalado como responsables de múltiples ataques contra las redes de comunicaciones, los proveedores de servicios y dispositivos de internet como CISCO, Netgear, D-Link, así como el daño temporal de múltiples sistemas de infraestructura crítica dentro de su territorio[63] [64]. Estos grupos han adecuado los *exploits* de la NSA y otras vulnerabilidades conocidas[65], operando de manera similar a la hora de infiltrar los dispositivos de red troncales[66]. También habrían infiltrado redes gubernamentales, usándolas como punto de ataques a terceros en la región del Asia-Pacifico para sus operaciones de espionaje[67].

A las capacidades ciber ofensivas hay que sumarles el potencial para dañar físicamente a otros componentes de las redes: los 530 cables submarinos de fibra óptica que transportan el 99% de las comunicaciones de internet y telefonía global[68]. Atacar los cables de comunicación ha sido la norma de varios países durante conflictos militares, incluso en casos donde los propietarios de los cables no eran parte de estos[69]. Ejemplos recientes muestran cómo un corte limitado de un par de cables puede dañar la conectividad de millones de personas en varios continentes[70], afectar la provisión de servicios de internet como Google, Microsoft, Amazon [71] o directamente dejar a países sin internet, produciendo la caída de todos los servicios como correo, mensajería, bancos, comercio electrónico y demás.[72] [73]

Se sospecha que China podría cortar los cables submarinos que conectan a Taiwán[74] para degradar su estructura de Comando y Control, lo que también afectaría seriamente la economía de la isla, junto a la de países como Japón y

[61]Nakashima, Ellen. "Chinese hackers who breached Google gained access to sensitive data; U.S. officials say". En: Jonathan Stempel: https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html

[62]Kanno-Youngs, Zolan; Sanger, David E. "U.S. Accuses China of Hacking Microsoft". En: https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html

[63] CISA. "People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices". En: https://www.cisa.gov/uscert/ncas/alerts/aa22-158a

[64]CISA. "China". En: https://www.cisa.gov/uscert/china

[65] Greenberg, Andy. "China Hijacked an NSA Hacking Tool in 2014—and Used It for Years". En: https://www.wired.com/story/china-nsa-hacking-tool-epme-hijack/

[66] Cinpanu, Catalin. "China has been 'hijacking the vital internet backbone of western countries". En: https://www.zdnet.com/article/china-has-been-hijacking-the-vital-internet-backbone-of-western-countries/

[67] Lyngaas, Sean. "Chinese spies hop from one hacked government network to another in Asia Pacific, researchers say" En: https://www.cyberscoop.com/naikon-china-hacking-check-point-australia-vietnam/

[68] "Submarine Cable Frequently Asked Questions" En: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

[69]Fargher. James A."Attacks on undersea cables: a Victorian legacy". En: https://www.strifeblog.org/2016/04/12/attacks-on-undersea-cables-a-victorian-legacy/

[70]Peterson, Andrea. "https://therecord.media/submarine-cables-cut-egypt-disruption/". En: https://therecord.media/submarine-cables-cut-egypt-disruption/

[71]Moss, Sebastian. "AAE-1 cable cut causes widespread outages in Europe, East Africa, Middle East, and South Asia". En: https://www.datacenterdynamics.com/en/news/aae-1-cable-cut-causes-widespread-outages-in-europe-east-africa-middle-east-and-south-asia/

[72] Edward, Jim. "The internet's worst-case scenario finally happened in real life: An entire country was taken offline, and no one knows why". En: https://www.businessinsider.com/undersea-international-internet-cables-cut-in-africa-2018-4

[73]Al Jazeera. "Tonga facing 'absolute disaster' after internet cable blackout". En: https://www.aljazeera.com/news/2019/1/23/tonga-facing-absolute-disaster-after-internet-cable-blackout

[74] Asia Sentinel. "Taiwan Fears China Could Cut Undersea Cables". En: https://www.asiasentinel.com/p/taiwan-fears-china-cut-undersea-cables?triedSigningIn=true

Corea del Sur[75]. También aplicar una parte del manual ruso en caso de un conflicto mayor[76]: apuntar a cortar los cables o atacar las conexiones físicas ubicadas en las estaciones de amarre de los cables[77] entre Estados Unidos y sus aliados[78]. En este escenario China tendría cierto nivel de protección, ya que la arquitectura de su internet estaría diseñada para desconectarse del mundo y seguir operando internamente en caso de ciberataques o intervenciones externas, de manera similar a la de Rusia[79].

Estados Unidos también tiene sus precedentes a la hora de atacar este tipo de infraestructura, cortando los cables de comunicación submarinos de Cuba y Filipinas durante su guerra con España, ya que los consideraba como objetivos legítimos[80] [81]. Durante la Guerra Fría, realizó intercepciones contra los cables submarinos de la Unión Soviética[82]. En la guerra de Irak de 2003, la infraestructura iraquí de internet fue destruida al inicio del conflicto[83] y recientemente, la NSA habría infiltrado regularmente las conexiones de fibra óptica de los principales operadores globales como Verizon, British Telecom, Vodafone, L3 Technologies[84] o Pacnet, uno de los mayores operadores de la región de Asia-Pacifico[85].

[75] NY Times. "How China could choke Taiwan". En: https://www.nytimes.com/interactive/2022/08/25/world/asia/china-taiwan-conflict-blockade.html?smid=tw-nytimes&smtyp=cur

[76] Sutton, H I. "How Russian Spy Submarines Can Interfere with Undersea Internet Cables". En: https://www.forbes.com/sites/hisutton/2020/08/19/how-russian-spy-submarines-can-interfere-with-undersea-internet-cables/?sh=49388a793b04

[77] Magnier, Mark. "Undersea internet cables a major vulnerability in any potential Taiwan attack, report finds". En: https://www.scmp.com/news/china/military/article/3190898/report-about-potential-attack-taiwan-focuses-vulnerability

[78] Durns, Sean. "Can China Compromise America's Undersea Cables?" En: https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/can-china-compromise-america%E2%80%99s

[79] Cimpanu, Catalin. "Oracle: China's internet is designed more like an intranet". En: https://www.zdnet.com/article/oracle-chinas-internet-is-designed-more-like-an-intranet/

[80] Harbin III, Dennis E. "Targeting Submarine Cables: New Approaches to the Law of Armed Conflict in Modern Warfare". En: https://tjaglcs.army.mil/mlr/targeting-submarine-cables-new-approaches-to-the-law-of-armed-conflict-in-modern-warfare

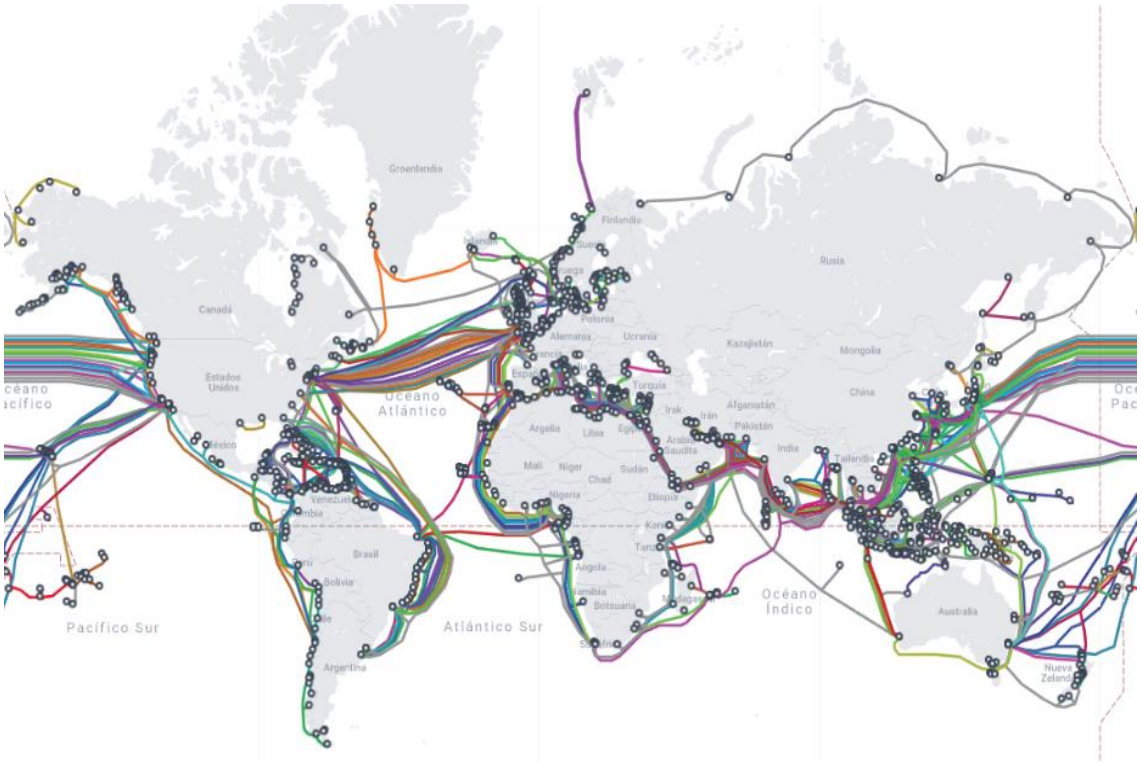
[81] Fargher. James A. Op. Cit.

[82] Military.com "The Mission Behind Operation Ivy Bells and How It Was Discovered". En: https://www.military.com/history/operation-ivy-bells.html

[83] Mcwilliams, Brian. "Iraq goes offline". En: https://www.salon.com/2003/03/31/iraq_offline/

[84] Perlroth, Nicole, Markoff, John. "N.S.A. May Have Hit Internet Companies at a Weak Spot". En: https://www.nytimes.com/2013/11/26/technology/a-peephole-for-the-nsa.html

[85] Lam, Lana. "EXCLUSIVE: US hacked Pacnet, Asia Pacific fibre-optic network operator, in 2009". En: https://www.scmp.com/news/hong-kong/article/1266875/exclusive-us-hacked-pacnet-asia-pacific-fibre-optic-network-operator




Mapa de Cables Submarinos[86]

**El posible daño colateral de los ciberataques y sabotajes sobre la Argentina**

En años recientes el Comité Internacional de la Cruz Roja (CICR) ha alertado sobre los posibles daños colaterales, afirmando que "el uso de ciber operaciones contra la infraestructura crítica tiene el riesgo de crear consecuencias humanitarias devastadoras"[87]. Parte de este problema está relacionado con la dificultad para discriminar entre blancos civiles y militares, ya que el uso dual de las redes de comunicaciones dificulta la posibilidad de restringir el daño a uno u otro sector. En muchos casos las redes militares pueden depender de la infraestructura civil, como los cables submarinos y los ruteadores para sus comunicaciones[88]. Esta situación es exacerbada en el caso de China con su política de "fusión civil-militar", que tiene como objetivo reforzar los nexos entre ambos sectores[89] y donde Huawei ha sido señalada como uno de los ejemplos de una empresa privada china con profundos lazos a los servicios de seguridad estatales[90].

En caso de un conflicto entre China y los Estados Unidos, es difícil saber hasta donde podrían primar los principios de proporcionalidad, así como el respeto de las reglas y convenciones que busquen mitigar el daño sus respectivas poblaciones civiles. Sin embargo, dado que este sería un conflicto por la

[86]https://www.submarinecablemap.com/
[87]Christory, Véronique. "ICRC calls on States to interpret rules to ensure adequate protection for civilians and civilian infrastructure, ICT systems and data". En: https://www.icrc.org/en/document/icrc-states-protection-civilians-data
[88]CICR. "International Humanitarian Law and Cyber Operations during Armed Conflicts". En: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts
[89] Kania, Elsa B; Laskai, Lorand."Myths and Realities of China's Military-Civil Fusion Strategy". En: https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy
[90] "Balding, Christopher. "Huawei Technologies' Links to Chinese State Security Services"". En: https://ssrn.com/abstract=3415726"

hegemonía global, la escalada progresiva podría empujar a ambos usar estas capacidades a gran escala.

En este conflicto, uno de los blancos más probables serían los servicios que son centrales para el funcionamiento de internet, como los mencionados IXPs, los Sistemas de Nombre de Dominio o *Domain Name System* (*DNS*), así como la afectación de los centros de datos de los principales proveedores de servicios de internet y todos los que dependan de estos,[91] mediante ataques de Denegación de Servicios Permanente (DoSP)[92] dirigidos a la destrucción del hardware físico[93] [94].

Cualquier propagación de malware diseñado para dañar equipos de red de fabricantes chinos podría tener consecuencias para la Argentina, ya que Huawei es el mayor proveedor de equipos para Telecom, Movistar y Claro[95], una situación similar al resto de los países de América latina[96], África[97] y Asia[98].

Si bien las redes como internet poseen redundancias que compensan por las caídas de servicio, es difícil prever la evolución de un escenario donde los principales IXPs y DNS que conectan a las diferentes redes entre Estados Unidos y sus aliados, estén bajo ciberataques sistemáticos, simultáneos y continuos con el uso de malwares específicamente diseñados para destruir el hardware de red, en conjunto con ataques a los cables submarinos. Los efectos combinados de estas operaciones podrían afectar a grandes porciones de internet, produciendo caídas prolongadas en la conectividad global por semanas o meses.

Nuestro país podría ser vulnerable en este escenario, ya que gran parte de los cables de Argentina y América Latina convergen en los Estados Unidos, en lo que se conoce como *Network Access Point* (*NAP*) *of the Americas* en la ciudad de Miami. Este es el centro neurálgico que contiene los DNS y al cuarto IXP en tamaño de los Estados Unidos, que interconecta a más de 120 redes globales y permite la comunicación entre 150 países[99]. Si bien existen otros cables intercontinentales redundantes que podrían redirigir parte del tráfico[100] por África

[91] CICR. "The potential human cost of cyber operations". En: https://www.icrc.org/en/document/potential-human-cost-cyber-operations
[92] TRG Datacenters. "What Is a Permanent DoS (PDoS) Attack and Can I Stop It?." En: https://www.trgdatacenters.com/what-is-a-permanent-dos-pdos-attack-and-can-i-stop-it/
[93] TrendMicro. "BrickerBot Malware Emerges, Permanently Bricks IoT Devices". En: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/brickerbot-malware-permanently-bricks-iot-devices
[94] Goodin, Dan. "A wide range of routers are under attack by new, unusually sophisticated malware". En: https://arstechnica.com/information-technology/2022/06/a-wide-range-of-routers-are-under-attack-by-new-unusually-sophisticated-malware
[95] Catalano, Andrés. "Dilema telco: Argentina depende de Huawei para redes 4G y 5G, en pleno conflicto China-Trump" En: https://www.iprofesional.com/tecnologia/293063-trump-vs-huawei-riesgo-para-movistar-personal-y-claro-en-argentina
[96] BNamericas. "How the US-Huawei cold war is playing out in Latin America". En: https://www.bnamericas.com/en/features/howtheushuaweicoldwarisplayingoutinlatinamerica
[97]DW. "Africa embraces Huawei technology despite security concerns". En: https://www.dw.com/en/africa-embraces-huawei-technology-despite-security-concerns/a-60665700
[98]Javad Heydarian, Richard. "SE Asia fragments on pro and anti-Huawei lines". En: https://asiatimes.com/2021/07/se-asia-fragments-on-pro-and-anti-huawei-lines/
[99]Dahlberg, Nancy. "Equinix buys 29 data centers from Verizon, including NAP of the Americas". En: https://www.miamiherald.com/news/business/technology/article147846254.html
[100] Hamblen, Matt "Cable cuts force rerouting of Internet traffic around the world". En: https://www.computerworld.com/article/2538937/cable-cuts-force-rerouting-of-internet-traffic-around-the-world.html

y Europa, la capacidad sería mucho más limitada, por lo que podría crearse una congestión de las comunicaciones en la infraestructura que quedara operativa.

A este escenario habría que sumarle potenciales restricciones resultantes de la priorización del uso de las redes de comunicaciones remanentes en manos de los Estados Unidos y sus aliados sobre el resto de los países, debido a las necesidades intensivas de datos e información que requieren sus fuerzas armadas para sus operaciones militares[101]. Un corte general de internet en Argentina afectaría a toda la población, las empresas y el gobierno, que dependen de ella para sus operaciones diarias.

Otro problema derivado es que ya existen casos de que cuando las vulnerabilidades que explotarían estos malwares se hacen conocidas, grupos criminales las explotan para realizar actividades delictivas[102]. Este es un riesgo extra que en una situación de conflicto entre China y los Estados Unidos puede ser agravado por la súbita desaparición de los servicios que estas empresas proveen para mantenerlos protegidos mediante actualizaciones de seguridad, así como proveer equipos de reemplazo.

A parte de la infraestructura de comunicaciones, las grandes empresas tecnológicas americanas, los proveedores de servicio de internet, así como las redes de distribución de contenidos, también pueden ser uno de los múltiples objetivos en un conflicto, donde China busque dañar la economía de los Estados Unidos mediante ciberataques[103]. En Argentina los servicios esenciales como infraestructura, mensajería, comercio electrónico, servicios en la nube y demás son provistos mayoritariamente por empresas norteamericanas como Cirion Technologies (infraestructura de red y fibra óptica), Google, Microsoft, Amazon, entre otras cuya provisión puede ser cortada por este tipo de ataques.

Existen otras empresas como Akamai Technologies o Fastly[104], que son Redes de Distribución de Contenidos, que optimizan el tráfico de internet y donde ya existen antecedentes de como la caída de los servicios de estos proveedores puede afectar la conectividad global y nacional: En julio de 2022, una falla mundial en los servidores de Akamai afectó a miles de páginas en Argentina, que incluían desde diarios, servicios de streaming, hasta comercio electrónico[105]. Un mes antes, otra caída esta vez de la empresa Fastly, dejo sin conexión a los servicios de mensajería como WhatsApp e Instagram[106]. Según un informe de la *Internet Society*, en años recientes se ha producido una concentración y una

[101] Hartman, Kim; Giles, Keir "Net Neutrality in the Context of Cyber Warfare". En: https://ieeexplore.ieee.org/document/8405015

[102] Arghire, Ionut. "Botnet's Huawei Router Exploit Code Now Public". En: https://www.securityweek.com/botnets-huawei-router-exploit-code-now-public

[103] Carnegie Endowment for International Peace. "Preventing Chinese Sabotage in a Crisis". En: https://carnegieendowment.org/2022/04/25/preventing-chinese-sabotage-in-crisis-pub-86922

[104] Chalmers, Stephanie. "Content delivery networks hope you've never heard of them — but if there's an outage, it's big news". En: https://www.abc.net.au/news/2021-08-12/content-delivery-networks-cyber-security-provider-outage-risks/10036762

[105] La Nación. "Caída de sitios: Akamai reveló la razón por la que buena parte de internet estuvo inaccesible hoy al mediodía" En: https://www.lanacion.com.ar/tecnologia/caida-de-sitios-por-que-dejo-de-funcionar-internet-hoy-al-mediodia-nid22072021/

[106] La Nación. "Qué es Fastly, la empresa detrás de la caída de sitios web a nivel mundial" En: https://www.lanacion.com.ar/el-mundo/que-es-fastly-la-empresa-detras-de-la-caida-de-sitios-web-a-nivel-mundial-nid08062021/

creciente interdependencia entre estas redes que pueden crear un efecto dominó para otras partes de la economía global[107] en caso de que estos fallarán.

## La dependencia de los Sistemas de Posicionamiento Global y su posible impacto en Argentina

A los escenarios de ciberguerra y el corte de cables submarinos hay que sumarle el potencial daño que puede ser producido por la guerra espacial. Las fuerzas norteamericanas son dependientes de la red de satélites de comunicaciones y de observación electroóptica[108] que le permiten realizar una variedad de operaciones como la vigilancia e inteligencia, el comando, control y comunicaciones de sus fuerzas militares. Más importante aún son los satélites del Sistema de Posicionamiento Global (GPS) de las cuales dependen la mayoría de sus plataformas de combate y municiones de precisión, así como el sostenimiento logístico de sus operaciones a escala global [109] [110].

En caso de un conflicto con China, dicha infraestructura podría ser el blanco principal de las operaciones militares chinas. Su ejército ha desarrollado una serie de capacidades que incluyen sistemas de guerra electrónica, misiles antisatélite, armas cinéticas y de energía dirigida[111], para "destruir, dañar e interferir con las capacidades enemigas de reconocimiento, observación y comunicación, así como navegación y alerta temprana" en las primeras etapas de un conflicto[112].

El peor escenario es que en un conflicto ocurra un ataque[113] generalizado en contra de la red de satélites de GPS. Un estudio[114] de la *Goverment Accountability Office* (GAO) determinó que al menos 16 sectores de la economía norteamericana dependen de los servicios de sincronización temporal de los GPS para su correcto funcionamiento[115]. Los servicios críticos cuya afectación sería la más destructiva son las redes de generación y distribución eléctrica[116]; las redes de comunicación[117]; los servicios de telefonía móvil y futuras redes

[107] Internet Society. "Internet Society Global Internet Report: Consolidation in the Internet Economy". En: https://future.internetsociety.org/2019/wp-content/uploads/sites/2/2019/04/InternetSociety-GlobalInternetReport-ConsolidationintheInternetEconomy.pdf p.48-49

[108] "Space Operations". En: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

[109] Barbier, reid. "The purpose and mission of the space force". En: https://www.american.edu/sis/centers/security-technology/the-purpose-and-mission-of-the-space-force.cfm

[110] "US military must avoid a 'kasserine pass' failure for space power". En: https://www.c4isrnet.com/opinion/2021/07/19/us-military-must-avoid-a-kasserine-pass-failure-for-space-power/

[111] Erwin, Sandra. "DoD: China amassing arsenal of anti-satellite weapons" en: https://www.realcleardefense.com/2020/09/02/dod_china_amassing_arsenal_of_anti-satellite_weapons_576126.html

[112] "Military power of the people's republic of China 2009". En: https://www.globalsecurity.org/military/library/report/2009/090324-dod-china-report/090324-dod-china-report.pdf

[113] Menn, Joseph. "China-based campaign breached satellite, defense companies: Symantec". En: https://www.reuters.com/article/us-china-usa-cyber/china-based-campaign-breached-satellite-defense-companies-symantec-idUSKBN1JF2X0

[114] GAO. "Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced". En: https://www.gao.gov/assets/gao-14-15.pdf

[115] "Timing". En: https://www.gps.gov/applications/timing/

[116] Shepard, Daniel P. "Going Up Against Time: The Power Grid's Vulnerability to GPS Spoofing Attacks". En: https://www.gpsworld.com/wirelessinfrastructuregoing-against-time-13278/

[117] Masterclock. "How Does GPS Network Time Synchronization Work?" En: https://www.masterclock.com/support/library/gps-network-time-synchronization

5G[118]; así como el sistema financiero[119] y la logística[120]; entre otros. Si bien existen capacidades de redundancia para compensar por fallos transitorios, sólo pueden operar por cortos periodos de tiempo[121], por lo que un corte total de los GPS durante 30 días, como mínimo produciría pérdidas por 45.000 millones de dólares sólo en los Estados Unidos[122].

Otro problema que puede generarse de la destrucción de algunos satélites es lo que se denomina el síndrome de Kessler[123]: cada destrucción de un satélite en la órbita terrestre por un misil antisatélite, crea una nube de restos espaciales que se desplaza a gran velocidad[124] y a su vez estos restos impactan a otros satélites, creando una reacción en cadena que puede llevar a la destrucción de la mayoría de los satélites en órbita e incluso crear una barrera de restos que pueda bloquear el futuro acceso al espacio de cualquier país[125].

Un escenario que afecte a los sistemas de posicionamiento global tendrá efectos más allá de los contendientes. En Argentina, las redes de generación y distribución de energía eléctrica, Internet, la telefonía celular, transacciones financieras, entre otras son dependientes del GPS para mantener sus operaciones[126]. De este grupo, las redes de generación y distribución eléctrica son una infraestructura crítica cuya afectación puede ser la más perjudicial. Este escenario podría ser una repetición del apagón del 16 junio de 2019, donde se produjo una totalidad de la falla en el territorio nacional de manera simultánea[127], sin embargo, en esta situación aún funcionaban las redes de celulares[128]. En este caso las redes móviles y los servicios de internet también serían afectados, por lo que en un escenario de caídas simultaneas y prolongadas de estos servicios, es posible que los esfuerzos para coordinar la respuesta a nivel nacional se vean seriamente degradados.

## La posibilidad de que acciones militares directas entre las potencias afecten a la Argentina

Este trabajo se ha focalizado en los daños colaterales de un conflicto entre China y Estados Unidos, independientemente de las definiciones de política exterior que Argentina adopte, y que serían comunes a una gran cantidad de países del

---

[118] "Satellite Synchronization is Critical to 5G Mobile Cellular Network Operation". En: https://www.viavisolutions.com/en-us/literature/satellite-synchronization-critical-5g-mobile-cellular-network-operation-white-papers-books-en.pdf

[119] Fernholz, Tim. "The entire global financial system depends on GPS, and it's shockingly vulnerable to attack". En: https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack/

[120] Dunn, Katherine. "Mysterious GPS outages are wracking the shipping industry". En: https://fortune.com/longform/gps-outages-maritime-shipping-industry/

[121] Glass, Dan. "What Happens If GPS Fails? En: https://www.theatlantic.com/technology/archive/2016/06/what-happens-if-gps-fails/486824/

[122] Reichmann, Kelsey. "30-day GPS outage could cost US industry $45B". En: https://www.c4isrnet.com/battlefield-tech/space/2019/06/17/30-day-gps-outage-could-cost-us-industry-45-billion/

[123] Clarín. "Qué es el Síndrome de Kessler, la nueva amenaza que pone en riesgo al planeta tras el coronavirus" En: https://www.clarin.com/internacional/sindrome-kessler-nueva-amenaza-pone-riesgo-planeta-coronavirus_0_zphF6xDSi.html

[124] Shachtman, Noah. "How China Loses the Coming Space War (Pt. 1)". En: https://www.wired.com/2008/01/inside-the-chin/

[125] Malekos Smith, Zhanna. "When elephants fight in space". En: https://aerospace.csis.org/the-problem-of-orbital-debris/

[126] "Generación de patrones de tiempo ultraestables". En: https://www.argentina.gob.ar/noticias/generacion-de-patrones-de-tiempo-ultraestables-3

[127] Histórico apagón en Argentina: el país entero sin luz". En: https://www.infobae.com/sociedad/2019/06/16/masivo-apagon-a-nivel-pais-capital-federal-buenos-aires-y-varias-provincia-estan-sin-luz/

[128] Jaimovich, Desirée. "Apagón: cómo funcionan las redes de telefonía móvil y por qué no nos quedamos sin señal". En: https://www.infobae.com/america/tecno/2019/06/16/apagon-como-funcionan-las-redes-de-telefonia-movil-y-por-que-no-nos-quedamos-sin-senal/

mundo. Se ha puesto de manifiesto, sin embargo, que urge desarrollar una estrategia diplomática que permita acomodar las demandas cruzadas que enfrentaría el país.

La Argentina cuenta con dos focos de atención que podrían entrar en juego en caso de una competencia militar entre las potencias. El primero se relaciona con la Estación de Espacio Lejano que la República Popular China tiene emplazada en Neuquén y cómo su uso militar contra los satélites americanos o de sus aliados en un conflicto[129] podría derivar en acciones militares punitivas dentro del territorio de nuestro país.

El segundo tiene que ver con las inversiones chinas en puertos a lo largo del mundo que podrían tener capacidad de uso dual[130]. Aunque aún no se han hecho realidad las advertencias del Comando Sur sobre inversiones chinas en el Polo Logístico Antártico en Tierra del Fuego, la posibilidad de que éstas se concreten, dentro de determinados parámetros de potencial uso militar, pondría a la Argentina en el escenario de una competencia entre las potencias. En caso de que Estados Unidos realice operaciones de bloqueo naval contra China, el Pasaje de Drake podría convertirse en un escenario de alta importancia estratégica para China[131], como vía alternativa de abastecimiento para convoyes y sus escoltas que busquen romper el bloqueo. Esta situación podría escalar rápidamente si las fuerzas norteamericanas o del Reino Unido posicionadas en las Malvinas intentaran hacer efectivo el bloqueo.

## Consideraciones finales

Estos ejemplos requerirán estudios en profundidad de los potenciales impactos, así como un análisis sistemático de las dependencias externas para desarrollar políticas dentro de un marco estratégico integral que ayude a atenuarlos.

Debido al alto grado de vulnerabilidad en el que se encuentra el país, es posible que muchos de estos impactos no puedan ser prevenidos, pero al menos se debería apuntar a lograr la continuidad operativa de los sectores críticos, que son el sostén de la sociedad en su conjunto. Entre las medidas se podrían incluir la protección de las reservas estratégicas de insumos para mantener en funcionamiento sectores vitales como alimentación, energía, salud e infraestructuras críticas, entre otros.

Al mismo tiempo, sería necesario reforzar las capacidades de ciberdefensa, ciberseguridad y examinar la posibilidad de desarrollar o invertir en sistemas que puedan funcionar como alternativas al GPS.

Finalmente, la necesidad de invertir en ampliar las capacidades de comando, control, comunicaciones, logística, movilidad táctica y estratégica, para las

[129] Seligman, Lara. “U.S. Military Warns of Threat From Chinese-Run Space Station in Argentina”. En: https://foreignpolicy.com/2019/02/08/us-military-warns-of-threat-from-chinese-run-space-station-in-argentina/

[130] Elizondo, Silvana. “los puertos de capitales chinos en el indo pacífico y más allá: qué características deben tener para un posible uso dual”. En: https://www.esgcffaa.edu.ar/maresdechina/boletin/boletin12-0607-2022_Analisis%20-%20Los%20puertos%20de%20capitales%20chinos%20-%20Silvana%20Elizondo.pdf

[131] Evan Ellis, Robert. “China’s Strategic Military Advance in Argentina”. En: http://chinayamericalatina.com/china-y-su-avance-militar-estrategico-en-argentina/

operaciones de apoyo a la comunidad de las Fuerzas Armadas, ya que son las únicas con la posibilidad de operar en forma inmediata a lo largo y ancho del país.