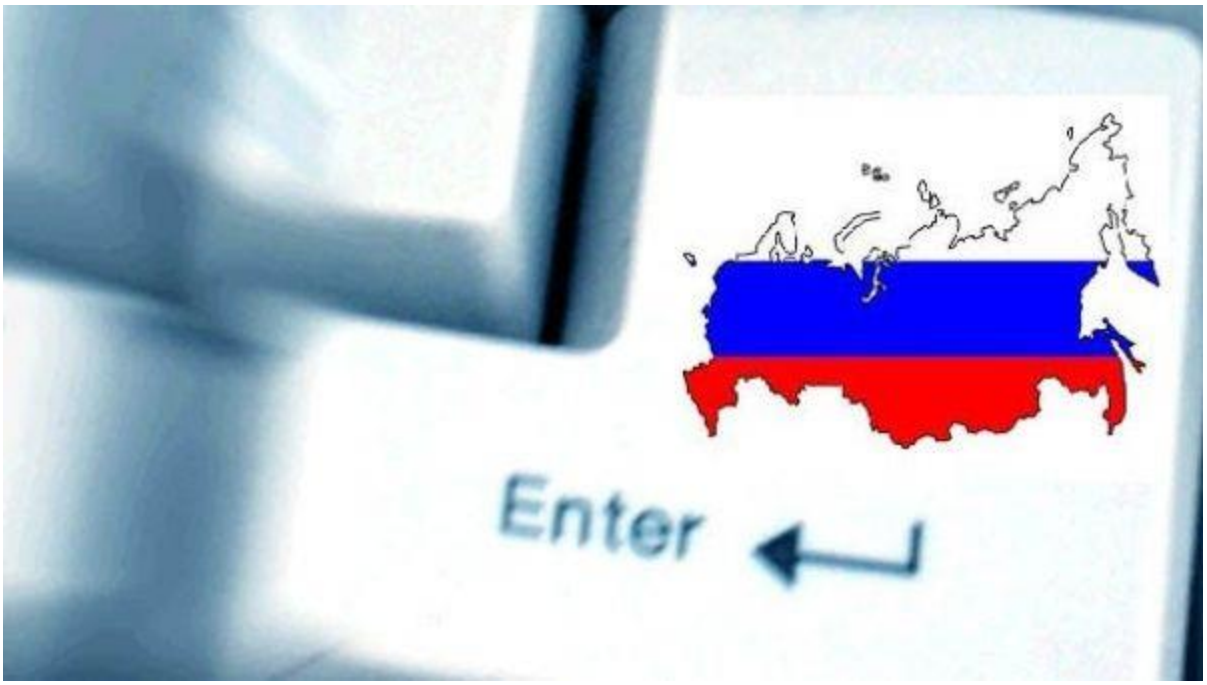
Todas las ciber-autopistas conducen a Rusia



(Fuente de imagen: Telesur, 2014)

Por: Andrés Gaitán Rodríguez

Textos de historia nos han enseñado que, durante sus casi quinientos años de vida (a partir del 27 a.C.), el Gran Imperio Romano cimentó caminos a lo largo de Europa y parte del norte de África en su calidad de hegemón de la época. Se relata que, aunque la mayoría de ocasiones estas vías fueron erigidas por arquitectos e ingenieros, en otros momentos, estas conexiones aparecieron espontáneamente con el paso de la "legión del águila" en sus carros, caballos y con su marcha cuando iban hacia las provincias o nuevos territorios por conquistar. Estos caminos, más allá de constituirse como senderos para ir de un lugar a otro, se instituyeron como hilos de poder garantes del control político y militar del centro hacia la periferia. De esta imagen del pasado devino la expresión, "todos los caminos conducen a Roma".

En la actualidad podríamos tomar las acciones hostiles que ha llevado a cabo la Federación Rusa en contra de otros Estados, a través del ciberespacio como el fundamento para extrapolar la frase creada para Roma hacia dicho actor. Aunque la escritura de este documento se enmarque dentro de un ejercicio académico que no demande la postulación de una tesis en un sentido científico, se permite a continuación expresar algunos argumentos que permitirían validar, por qué, bajo las circunstancias actuales en las que Rusia se ha posicionado como potencia militar y de espionaje ciberespacial, tendría cabida la analogía, "todas las ciber-autopistas conducen a Rusia".

Es interesante pensar, como lo relata Jeffrey Carr en su libro *Inside Cyber Warfare*, cómo la Federación Rusa ha constituido en los últimos veinte años cibercapacidades, para potenciar su poder en materia de política exterior (CARR, 2010). Con el objeto de alcanzar sus Intereses, ésta Nación, creando unidades militares y de inteligencia especializadas en explotar las características estratégicas y furtivas del ciberespacio, ya ha violado el principio de soberanía de diversos actores del sistema internacional; principalmente, la de los países que sustentan alguna relación con la extinta Unión Soviética. En amabas situaciones (global y regional), eventos como, la intervención en el ejercicio electoral de los Estados Unidos de Norteamérica durante sus últimas elecciones presidenciales, o bien, las embestidas a Ucrania desatadas desde el incidente de Crimea hasta los imperantes levantamientos de las provincias de Donetsk, Luhansk y Járkov nos dice que este es un fenómeno coyuntural que denota su realidad y urgencia analítica.

Desde lo militar, el ciberataque o ciberespionaje se consideran revolucionarios como forma de combate puesto que, y como lo validaría una autoridad en el tema como Martin C. Libicki, se pueden proyectar a cualquier objetivo o sistema informático de nivel estatal, organizacional y personal independientemente su ubicación en el planeta, siempre y cuando, este cuente con una conexión a la Red. Son tácticas y armas diferenciales pues doblegan las barreras del tiempo y espacio a la que las Fuerzas tradicionales de acción en tierra, mar y aire no se pueden desprender; o por lo menos en un sentido estricto, pues hoy en día su funcionamiento también está integrado a las tecnologías de la información y la comunicación (LIBICKI, 2009). Es una idea que se fundamenta principalmente en el "dónde" y no en el "cómo", pues ya han emergido Instituciones militares con jurisdicción única y especial en el ciberespacio; para el caso que nos ocupa, las "*Information Troops*" y el "*APT 28 Group*", (que también se denominan "*Fancy Bear*" o "*Strontrium*")[1].

Haciendo un análisis ligero del resultado de los sucesos internacionales en donde se vinculó a Rusia, es posible sintetizar que, las "*Information Troops*" poseen el poder de acceder a sistemas informáticos críticos, como los Sistemas de Control Distribuido (DCS) y los Sistemas de Control Industrial (ICS) que permiten automatizar procesos como, el control de tráfico de vehículos (aéreos, marítimos y ferroviarios), de la refrigeración de los reactores nucleares, del alza y baja de los precios en las bolsas de valores, de los mecanismo de encendido y apagado de las redes energéticas, así como otros servicios vitales para una sociedad. También pueden atacar servidores DNS (*Domain Name System*) de tipo "*.gov*" y "*.mil*"; servidores en donde usualmente funcionan las páginas web empleadas organismos gubernamentales y defensa. No se quedan por afuera las filtraciones a tecnologías de tipo *cloud storage* y de almacenamiento empleados por el sector público y sus contratistas privados para guardar información de carácter secreta.

Al respecto, y concentrándonos en los acontecimientos de los últimos días. El diario *The Independent* dio a conocer pocos días tras cómo el *Government Communications Headquarters (GCHQ)* del Reino Unido advirtió a los líderes de los partidos políticos que los sistemas informáticos como e-mails y páginas web comprometidas con la labor democrática del Gobierno podría estar amenazada por los ciberataques rusos; no obstante, tanques de pensamiento y grupos de presión también han estado en la mira (INDEPENDENT, 2017). La cadena ABC informó recientemente que Rusia había hackeado miles de cuentas de correo electrónico de Yahoo que pertenecían a Oficiales del Gobierno de Estados Unidos (ABC, 2017). The Guardian registró cómo desde este mismo país se infiltró las cuentas de correo de los más importantes miembros del servicio diplomático de la República Checa (THE GUARDIAN, 2017).

Por su parte, para Reuters fue significativo el hecho de que Alemania denunciara que el aumento de la propaganda rusa en Internet son ciber-ataques camuflados (REUTERS, 2017). Bastante ilustrativo la denuncia que llevó a cabo el *United States Computer Emergency Readiness Team* (adscrito al Department Of Homeland Security (DHS) y a la Oficina del Director Nacional de Inteligencia) con relación a cómo Rusia comprometió la seguridad del proceso electoral en donde el actual Presidente, Donald Trump, fue electo (US-CERT, 2016).

En esta materia, es claro que nuestro actor en estudio ha constituido hilos de control, sobre procesos políticos soberanos de otros Gobiernos mediante soldados y armas capaces de transitar las ciber-autopistas. Ya que los casos enunciados involucran a países avanzados en esta materia, por lo que poseen recursos para detectar la ejecución de agresiones, y proponer contingencias; cabría preguntarse qué estará pasando con la seguridad y el Derecho a la no Intervención de los países atrasados o emergentes en ciberseguridad y ciberdefensa y que, por ende, no puedan percatarse de los mecanismos superiores empleados por los rusos (y en realidad cualquier Estado con las capacidades para hacerlo) para penetrar sus sistemas críticos con fines políticos.

Los escenarios y efectos más devastadores de este poder los han tenido que afrontar los Estados más cercanos a la Potencia. Como para el Imperio Romano fueron sus senderos, las ciber-autopistas, han servido para la consolidación de un poder hegemónico sobre los actores políticos que estén en su órbita de influencia regional; no cabe duda que, los Estados que pertenecieron o surgieron posteriormente a la URSS, desde 1991 hasta nuestros días, no han sido beneficiarios de un verdadero estatus de independencia. Para la Federación Rusa, lo "ciber" significa el medio, o bien el complemento, para lograr una política expansionista efectiva y eficiente. Aunque aprovechando tecnología que brotó de la cuarta revolución industrial (la informática y cibernética), Vladímir Putin, en calidad de Presidente, ha ordenado la ejecución de operaciones militares que combinan el despliegue de tropas en el terreno y el despliegue de ciberataques para alcanzar objetivos en materia de control geopolítico.

En abril del 2007, Rusia generó el ciberataque más catastrófico que se había registrado en el sistema internacional en contra de la República de Estonia. Las razones políticas se atribuyeron al traslado de lugar de un monumento soviético de la Segunda Guerra Mundial ubicado en Tallin, y el resultado fue un ciberataque masivo contra toda la infraestructura informática del gobierno, del sistema bancario, financiero, la red de comunicaciones y los medios informativos del país. En junio de 2008, el turno sería para Lituania cuando su Gobierno intentó rechazar los símbolos soviéticos. En agosto del mismo año, Georgia recibiría el primer ataque combinado por parte de Rusia. Después de que el gobierno pro-occidental electo en dicho Estado decidiera hacer frente militar terrestre, por mar y aire sobre las fronteras para contener el expansionismo ruso, los hackers rusos actuaron para deshabilitar todas las comunicaciones internas del país, mientras que las tropas en sus tanques comandadas desde el Kremlin invadían parte de Osetia del Norte; a su vecino (NBC NEWS, 2017).

Presentando motivaciones y *modus operandi* similares, algunos de los acontecimientos de la campaña ciberespacial rusa a nivel regional se podrían resumir así: 2009 Kirguistán; 2009 Kazajistán; 2009, segundo ataque a Georgia; 2014 en Ucrania días después a la elecciones presidenciales en donde se da un cambio hacia una perspectiva geopolítica occidental después de la revolución naranja; 2014, nuevamente Georgia; 2015, Ucrania; y en 2016, Crimea (NBC NEWS, 2017).

Para finalizar una reflexión respecto a "todas las ciber-autopistas conducen a Rusia". A diferencia del posible rastreo que se puede ejercer sobre el armamento cinético tradicional (misiles, bombas, fusiles, tanques, etc); así, como la constatación de evidencia del ejercicio de un ataque militar territorial, la mayoría de ciberataques o espionaje a través del ciberespacio no es perceptible. Por esto, la decisión y voluntad política de los Estados que ejercen estas acciones en contra de otros denota un comportamiento autoritario de carácter estatal. Y se apela al concepto de "comportamiento autoritario de carácter estatal", pues se trata de un fenómeno de las Relaciones Internacionales; ya no se trata de autoritarismo de un gobierno contra su sociedad, se trata de despotismo Estado-Estado. Al respecto, y en alusión a los incidentes en donde su país se ha visto atacado, el expresidente de Estonia, Tomas Hendrik Ilves, declaró hace pocos días:

Russia is engaging in asymmetrical warfare. It's asymmetrical because they can do things to democracies that democracies can't do back to an authoritarian government.

Notas al pie de página:

[1] Podemos encontrar otros referentes sobre la conformación de cuerpos estatales operacionales en el ciberespacio como, el *U.S Cyber Command*, el Comando Conjunto de la Fuerzas Militares de Colombia, y la Unidad 61398 del Ejército Popular de Liberación de China, entre otros.

Referencias

CARR, Jeffrey. Inside Cyber Warfare. O'Reilly Media 2010. Sebastopol

LEVINE, Mike y SHAPIRO, Emily. How Russian agents allegedly directed massive

Yahoo cyberattack. ABC NEWS, 2017. Consultado en: http://abcnews.go.com/US/russian-agents-facing-charges-yahoo-hacking-attacks/story?id=46142396

Martin C. Libicky. Military Cyberpower. En: KRAMER, Franklin. Cyberpower and National Security. National University Defense Press y Potomac Books. Dulles. 2009

OSBORNE, Samuel. UK political parties at risk from Russian cyber-attacks, GCHQ warns. The Independent, 2017. Consultado en: http://www.independent.co.uk/news/uk/politics/gchq-russian-hacking-cyber-attack-threat-uk-political-parties-general-election-threat-kremlin-a7625226.html

SHALAL, Andrea y SIEBOLD, Sabine. Germany sees rise in Russian propaganda, cyber attacks. REUTERS, 2017. Consultado en: http://www.reuters.com/article/us-germany-russia-idUSKBN13X15D

TAIT, Robert. Czech cyber-attack: Russia suspected of hacking diplomats' emails. The Gardian, 2017. Consultado en: https://www.theguardian.com/world/2017/jan/31/czech-cyber-attack-russia-suspected-of-hacking-diplomats-emails

THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER (NCCIC). GRIZZLY STEPPE – Russian Malicious Cyber Activity Report. NCCIC y FBI. 2016

WINDREMROBERT, Robert. Timeline: Ten Years of Russian Cyber Attacks on Other Nations. NBC News, 2017. Consultado en: http://www.nbcnews.com/news/us-news/timeline-ten-years-russian-cyber-attacks-other-nations-n697111