Into the breach. Defence companies target the cyber-security market. Demand for cyber-products is growing at twice the rate of that for military hardware

Enviado por Francisco Desentis en Vie, 08/10/2018 - 13:48
Cita:

The Economist [2018], "Into the breach. Defence companies target the cyber-security market. Demand for cyber-products is growing at twice the rate of that for military hardware", *The Economist*, London, 28 de julio, https://www.economist.com/business/2018/07/26/defence-companies-target-t... [1]

Fuente:
The Economist
Fecha de publicación:
Jueves, Julio 26, 2018
Revista descriptores:
Corporaciones militares - corporaciones civiles que participan en la producción militar o en actividades militares [2]
Relación economía y guerra [3]
Relaciones entre empresas estados y sociedad [4]
Sujetos de la guerra [5]
Tecnologías militares - tecnologías de uso dual [6]
Tema:
Las empresas de defensa prestan atención al mercado de ciberseguridad militar y civil
Idea principal:

Los ataques cibernéticos están a la orden del día tanto contra las estructuras militares como en la sociedad civil. Es una situación que compete a los gobiernos, al sector empresarial y, particularmente, a las empresas de defensa.

The Economist muestra las evidencias en estadísticas. Tan sólo en 13 años se incrementó sustancialmente el mercado de ciberseguridad militar y civil pasando de 3.5 mil millones de dólares en 2004 a 120 mil millones de dólares en 2017. Asimismo, según estimaciones de la empresa de investigación Cybersecurity Ventures, dicho mercado mantendrá una tendencia expansiva de entre 12% y 15% anual en los próximos tres años, esto es, el doble del monto global presupuestado para la compra de equipo de defensa.

Gran parte de todo esto se debe al contexto de los ataques cibernéticos rusos contra Occidente. Tanto el Congreso estadounidense como el Ministerio de Defensa de Reino Unido han asignado presupuesto a la detección y anulación de amenazas cibernéticas. Las empresas privadas, por su parte, siempre han incluido gastos de este tipo para cubrir cuestiones de ciberseguridad.

El caso de las empresas de defensa es muy particular. Por un lado, desde la década de los años noventa, cuando se popularizó el internet, se encuentran protegiendo sus armas y sistemas tecnológicos de información de todo posible ataque de ciberseguridad; por otro lado, desde hace aproximadamente diez años se han ocupado de ofrecer servicios de ciberseguridad a los gobiernos y empresas privadas, pero el negocio no tuvo los rendimientos esperados.

Resulta que el mercado de ciberseguridad tiene una variedad de 3 000 empresas distintas, en comparación con las escasas diez firmas existentes para ensamblar aviones militares. Las empresas de defensa no supieron, afirma el semanario inglés, entablar relaciones comerciales con empresas privadas de ciclos cortos de compra ni hacer frente a las empresas tecnológicas que desarrollan mejor el servicio que se empeñaron en ofrecer, a saber, software creador de murallas protectoras. Por ello algunas empresas de defensa prefirieron regresar al mercado de las armas convencionales al percibir un auge en el sector; según IHS Markit, una empresa de investigación, los presupuestos militares globales del año 2018 van a alcanzar una cifra récord desde la guerra fría.

No obstante, existen casos de empresas de defensa con altos rendimientos cuya estrategia ha sido básicamente por dos vías: la experiencia de la propia firma en actividades de ciberseguridad o la compra de otras firmas especializadas en ello. En efecto, por un lado la alta demanda de servicios de seguridad ha sido favorable para las empresas de defensa con experiencia en identificación activa de amenazas y planeación de estrategias resolutivas; la experiencia militar de estas empresas jugó a su favor para ganar la preferencia de los gobiernos y de algunas empresas privadas que sufren grandes ataques a su ciberseguridad. Por otro lado, está la situación de las adquisiciones; en abril de 2018 General Dynamics compró por 9.7 mil millones de dólares a CSRA, una empresa especialista en ciberseguridad, para colocarse como el principal proveedor de servicios de tecnología de información del gobierno de Estados Unidos o también están los casos de la inversión de Lockheed en empresas emergentes como Cybereason, especialista en inteligencia artificial, y L3 Technologies, otro grupo de defensa estadounidense.

Este auge de los servicios de ciberseguridad ha provocado duras advertencias en contra de las empresas que únicamente producen armas convencionales, al punto que algunos funcionarios estadounidenses piensan retirar contratos a aquellas empresas que consideren vulnerables a los ataques cibernéticos. El cambio de tono de advertencia a amenaza en contra las empresas productoras de armas se da por los casos recientes de ataques cibernéticos. Fue a principios de este año cuando China robó los planos estadounidenses de un misil antibuques supersónico de un contratista naval; BAE Systems, asesor del mayor grupo de defensa europeo, afirma que tendrá “serios problemas” para vender aviones y misiles a Arabia Saudita, su principal cliente, si pierde su división de inteligencia aplicada.

De alguna manera las principales empresas de defensa productoras de hardware buscan adelantarse ante las posibles disminuciones de la demanda ya que en 2020 termina el presupuesto asignado por Estados Unidos al rubro. Su apuesta es diversificar los servicios de ciberseguridad ya existentes, según afirma Frank Ford de la consultora Bain & Co. A diferencia del desplome de los presupuestos militares tras el fin de la guerra fría, la ciberseguridad parece menos volátil a una suspensión de operaciones.

Datos cruciales:

1. En 2015 Boeing vendió la empresa de sofware Narus a Symantec, una empresa rival.

2. En 2015 General Dynamics vendió Fidelis, la división cibernética comercial, a una empresa del sector privado.

Nexo con el tema que estudiamos:

La aguda expansión del mercado de los servicios de ciberseguridad con destino militar abona a la confirmación de la hipótesis del proyecto: “el poder de las corporaciones va de la mano de la centralidad de lo militar en el siglo XXI”. La disputa entre distintas empresas de defensa por consolidarse como el principal oferente de servicios de ciberseguridad a las arcas gubernamentales estadounidenses, rusas, chinas, etcétera, es tan sólo el preámbulo de la extensión de la guerra a niveles virtuales y cibernéticos. Se trata de servicios no sólo defensivos sino ofensivos que ponen en jaque a uno de los recursos más preciados y estratégicos para ejercer un control geopolítico de las regiones: la información.

En perspectiva micro-económica, observamos la dinámica entre el monopolio militar, la irrupción de las tecnologías de seguridad cibernética y la absorción de las empresas innovadoras por parte de las empresas líderes. Es preciso establecer los principales segmentos de esta actividad para conocer las tecnologías claves y las empresas que las generan y las controlan... Por otra parte, el carácter artesanal-casuístico de los ataques cibernéticos hace necesario el mantenimiento de nichos artesanales en que se recurre incluso a antiguos hackers y ciberdelincuentes que cambian de bando para obtener ventajas o reducir sus condenas judiciales.

Links
[1] https://www.economist.com/business/2018/07/26/defence-companies-target-the-cyber-security-market
[2] http://let.iiec.unam.mx/descriptores-let/corporaciones-militares-corporaciones-civiles-que-participan-en-la-producci%C3%B3n
[3] http://let.iiec.unam.mx/descriptores-let/relaci%C3%B3n-econom%C3%ADa-y-guerra
[4] http://let.iiec.unam.mx/taxonomy/term/20
[5] http://let.iiec.unam.mx/descriptores-let/sujetos-de-la-guerra
[6] http://let.iiec.unam.mx/descriptores-let/tecnolog%C3%ADas-militares-tecnolog%C3%ADas-de-uso-dual