Título Cibertucídides

Tipo de Producto Divulgación

Autores Rubbi, Lautaro

Publicado en: Estado Internacional

Código del Proyecto y Título del Proyecto

A17S28 - Ciberseguridad, Ciberguerra y Deep Web, las nuevas amenazas del Siglo XXI. Aproximación al caso chino 2010 - 2016

Responsable del Proyecto

Rubbi, Lautaro

Línea

Agenda Internacional

Área Temática

Ciencias Políticias y RRII

Fecha

Febrero 2017

INSOD
Instituto de Ciencias Sociales y Disciplinas Proyectuales

UADE Fundación UADE

Cibertucídides

Por Lautaro Rubbi, docente investigador
del Instituto de Ciencias Sociales de la Fundación
UADE – CONICET.

El antiguo y siempre presente dilema de seguridad se torna aún más complejo y peligroso cuando se aplica al ciberespacio.

Se ha popularizado en los últimos tiempos el concepto de la "trampa de Tucídides", que designa aquellos dilemas trágicos que llevarían a las grandes potencias a enfrentarse entre sí por mera cuestión de percepciones. En su famosa obra Tucídides escribía "fue el auge de Atenas y el miedo que ello inspiro en Esparta lo que hizo la guerra inevitable". Como demostró Graham Allison en un estudio reciente, el patrón se ha reiterado a lo largo de la historia: Cuando una Nación crece, especialmente mientras aumentan su seguridad, genera sentimientos de inseguridad y preocupación sobre otros, que toman la amenaza seriamente. Según el dilema de seguridad, el aumento de las defensas propias se percibe como armas de ataque para otros. Superarlo implica desarrollar medidas de fomento de la confianza y mucha comunicación, pero la percepción de amenaza nunca llega a ser nula.

Según el nuevo libro de Ben Buchanan, investigador de Harvard, el dilema se desarrolla de forma similar en el ciberespacio, aunque con divergencias que aumentan el peligro.

En primer lugar, desarrollar la capacidad para generar un daño significante y dirigido mediante ciber operaciones requiere enorme preparación. En otros tipos de conflicto, el desarrollo de las armas era hecho en territorio propio y luego desplegadas, pero las ciber operaciones son más complicadas. Desarrollar y probar una capacidad de ataque cibernética usualmente requiere ganar acceso al sistema objetivo por adelantado para lograr reconocimiento de las vulnerabilidades. En otras palabras, si un Estado desea ser capaz de atacar las redes de otra Nación, requiere comenzar a trabajar en esto con mucha anticipación, incluso si el desarrollo de esta capacidad se busca por razones de disuasión o planes de contingencia.

El problema surge cuando el Estado que sufre la intrusión lo detecta. Es difícil conocer las intenciones de otra Nación, especialmente en el ciberespacio, donde el lenguaje es confuso y la diferencia entre capacidades de ataque y defensa es escasa. Los políticos podrían concluir que la intrusión es el preludio a un ataque futuro, tal vez incluso a un ataque inminente. En tal caso podrían escalar la tensión o hasta tratar de atacar preventivamente.

Pero la intrusión en redes foráneas no solamente se puede hacer por cuestionesResultado de imagen para ciberseguridad disuasivas. También podría buscarse la penetración de los sistemas para detectar el desarrollo de sistemas de ataque. Conocer el arma del enemigo es la mejor forma de elaborar una buena defensa. Parte de esta lógica estuvo detrás de algunas de las operaciones reveladas por Edgar Snowden, como el acceso que logró la Agencia de Seguridad Nacional a computadoras chinas utilizadas para lanzar intrusiones sobre sistemas americanos, detectando

ataques pasados y objetivos futuros. Aún en este caso el dilema de seguridad se replica y hasta complica, pues no solo planes de contingencia ofensivos pueden ser interpretados como ataques, sino también operaciones que son genuinamente defensivas en su esencia. Tucídides se aplica: las malas interpretaciones pueden llevar a escalar en conflicto, aun cuando ningún participante quiera efectivamente hacer daño.

En suma, la Ciberseguridad plantea un nuevo dilema para los Estados. Tienen incentivos para penetrar redes extranjeras, sea para conducir ataques, para elaborar planes de contingencia y disuasión o para mejorar sus defensas. Pero la imposibilidad de detectar las verdaderas intenciones crea riesgos de malas interpretaciones y escalamiento. Esta posibilidad aumenta por el temor y desconocimiento sobre lo que la intrusión podría implicar, pues operaciones con muy variados objetivos y efectos pueden requerir grados similares de penetración. Mientras más naciones desarrollan ciber capacidades de defensa y ataque, el problema empeora. La trampa de Tucídides resurge y toma nuevas formas. Superarla requerirá medidas de confianza y mucha comunicación, pero también nuevas aproximaciones, pues no todos los antiguos métodos funcionaran por igual.

Artículo Publicado en:

https://www.estadointernacional.com/cibertucidides/