El papel de la ciberseguridad en el conflicto entre Rusia y Ucrania

*“El papel de la **ciberseguridad es clave en el conflicto Rusia-Ucrania y en el mundo en el que vivimos**”*, puntualizó **Gonzalo García- Belenguer Cuchi**, director del **Hub de Ciberseguridad** del **Tecnológico de Monterrey en Santa Fe.**

La **invasión de Rusia a Ucrania** comenzó el **24 de febrero de 2022** y forma parte de la **ciber guerra ruso-ucraniana comenzada en 2014,** en la que la **ciberseguridad** ha sido clave en el conflicto.

El especialista compartió que de hecho se podría decir que **este conflicto ha tenido ya varios capítulos de ciberguerra,** esto debido a que los **ataques cibernéticos** entre **Rusia y Ucrania** datan de 2014.

width="900" loading="lazy">

2014: ataque al sistema de elecciones

Los ataques o amenazas de ciberseguridad han sido persistentes de Rusia hacia Ucrania y de acuerdo con el académico comenzaron en 2014 al impactar su **sistema de elecciones.**

*“Afortunadamente **los ucranianos se dieron cuenta de lo que había pasado y no tuvo mayor repercusión**.*

*"Los rusos además hicieron **un ataque de denegación de servicios al sistema de conteo para retrasar la elección final**”*, recordó.

width="900" loading="lazy">

2015, 2016 y 2017: ataque al sistema eléctrico nacional

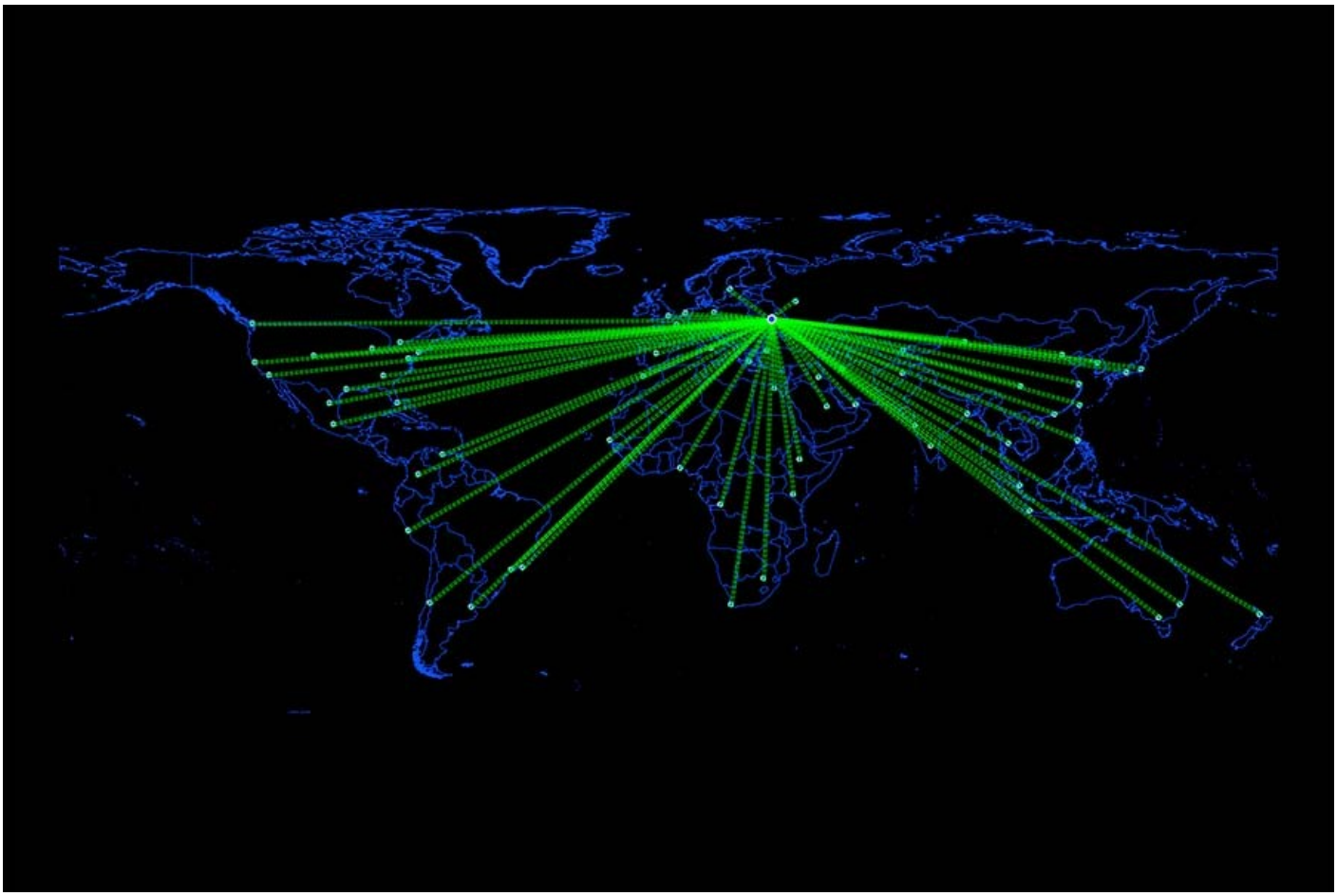
El director del **Hub de Ciberseguridad del Tec** comentó que en los episodios ocurridos en 2015, 2016 y 2017 al sistema eléctrico nacional de Ucrania se comprometieron **tres distribuidoras.**

“El malware (programa maligno) ***privaba de energía*** *y además no* ***permitía restaurar el sistema***”, señaló.

El especialista compartió que en este suceso se comprometió un subastador en la ciudad de **Kiev** y que el programa pernicioso además causó **daño físico a las máquinas,** además de privar de energía a la urbe**.**

“Usando NotPetya Ramsomware y wiper (códigos malignos) atacaron al sector energético, financiero y también al sector público como al privado.

Este ataque afectó al 80% de los sistemas en Ucrania *porque encriptaba el disco duro y lo dejaba* ***inutilizable e irrestaurable***”, puntualizó García- Belenguer.



width="900" loading="lazy">

Ciberseguridad y los ciberataques en el conflicto

Para el profesor del Tec este conflicto no solo se está dando en términos terrestres, aéreos y marítimos, sino que las estrategias van más allá de técnicas militares.

Dijo que en está lucha tiene un lugar importante el ciberespacio, esto con la intención de debilitar al enemigo y citó:

*“Cabe destacar que **los líderes ucranianos han pedido ayuda a sus hackers** para que luchen contra Rusia y así lo están haciendo. Se están atacando infraestructuras en Rusia, no solo por los hackers ucranianos sino también a nivel global”*.

"Los líderes ucranianos han pedido ayuda a sus hackers para que luchen contra Rusia y así lo están haciendo".

El titular del Hub de Ciberseguridad compartió que **las repercusiones pueden ser catastróficas si los hackers son exitosos y violentos** ya que las consecuencias de estos ciberataques impactarían no solamente a los países involucrados, sino a todo el mundo.

Explicó que algunas naciones pueden verse comprometidos, **afectar su economía, impacto en el mercado extranjero y por supuesto a las cadenas de suministro.**

width="900" loading="lazy">

Gonzalo García- Belenguer enfatizó en que es importante que se cuente con tácticas de ciberseguridad para controlar, manejar o eliminar estos riesgos.

“Los ataques a infraestructuras críticas ***pueden ser mortales para la población****, por ejemplo* ***provocar explosiones en centrales nucleares a través de un código malicioso.***

“Afortunadamente no hemos visto esto todavía y esperemos que siga así y que ***este conflicto acabe pronto****”*, *concluyó.*

SEGURO QUERRÁS LEER TAMBIÉN: