The role of cybersecurity in the conflict between Russia and Ukraine

“The role of ***cybersecurity is key in the Russia-Ukraine war and the world we live in,”*** stated **Gonzalo García- Belenguer Cuchi**, director of **Tecnológico de Monterrey’s cybersecurity hub in Santa Fe campus.**

Russia’s **invasion of Ukraine** began on **February 24, 2022,** and is part of the **Russia-Ukraine cyberwar that started in 2014. Cybersecurity** has been a key part of the conflict.

The specialist told us it might even be said that **this conflict has involved several stages of cyberwar** due to the fact that **cybernetic attacks** between **Russia and Ukraine** have been commonplace since 2014.

width="900" loading="lazy">

2014: attack on the electoral system

Russian threats or cybersecurity attacks on Ukraine have been persistent and, according to García- Belenguer, first took place in 2014 with the resulting adverse effects on the **electoral system.**

“Fortunately, ***the Ukrainians realized what was going on and there were no major repercussions****.*

“The Russians also orchestrated ***a denial-of-service attack on the counting system to delay the final election****,”* he recalled.

width="900" loading="lazy">

2015, 2016, and 2017: attack on the national electricity system

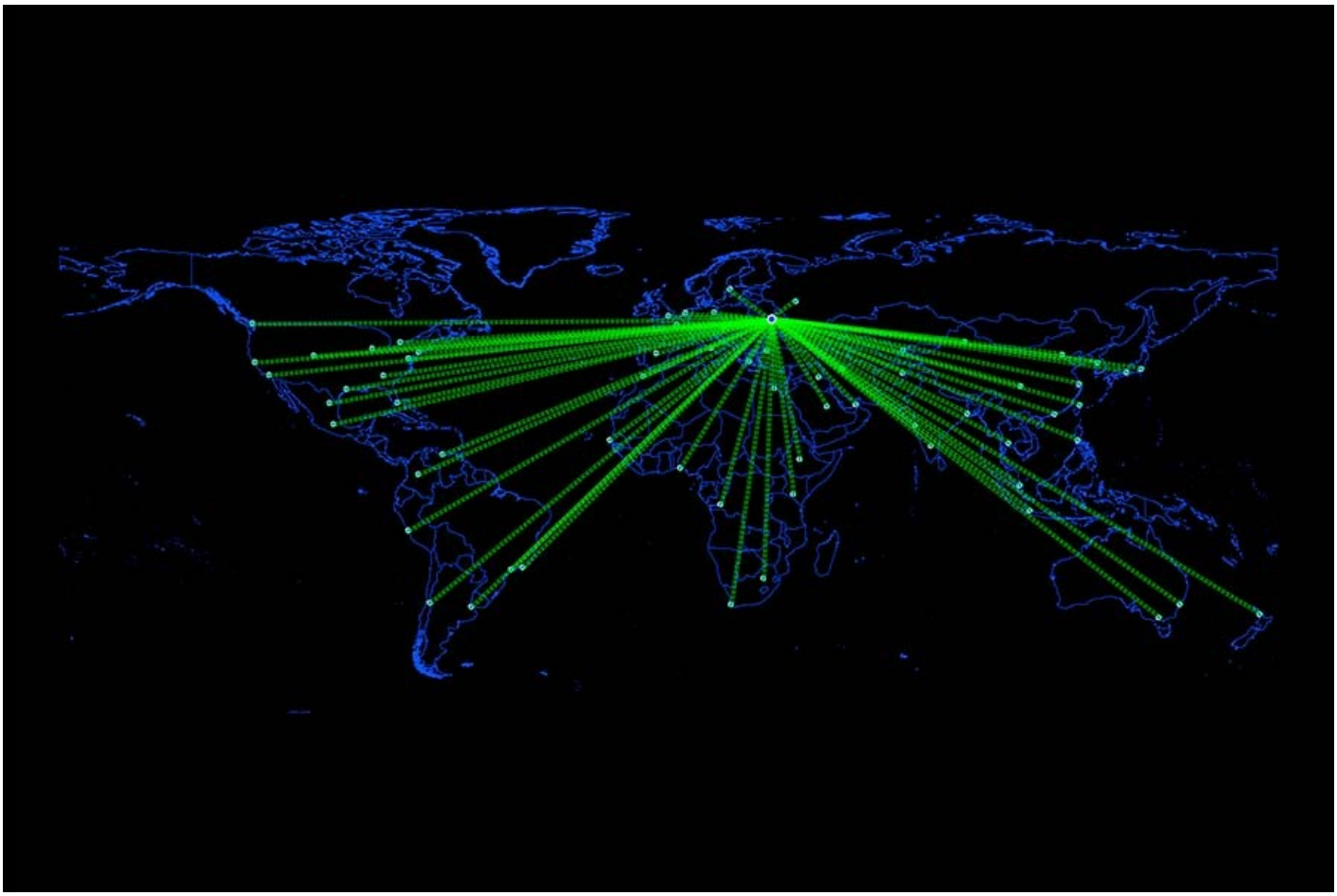
The Director of the **Tec's cybersecurity hub** said that these events took place in 2015, 2016, and 2017 and that **three of Ukraine's national electricity system distributors** were affected.

*"The malware **bled energy from the system** and **made it impossible to reset,**"* he said.

The specialist told us that this event adversely affected a substation in **Kyiv**, where the malicious software also **physically damaged the machines** in addition to cutting off the city's energy supply**.**

"Using the NotPetya wiper and ramsomware (malicious codes), they attacked both private and public energy and financial sectors.

***This attack affected 80% of Ukraine's systems** because it encrypted the hard drive and left it **unserviceable and impossible to reset,**"* asserted García- Belenguer.


width="900" loading="lazy">

Cybersecurity and cyberattacks during the conflict

According to the Tec professor, this conflict is not limited to the land, air, and sea; it also employs strategies that go beyond military interventions.

He said that this struggle occupies an important place in cyberspace and is designed to weaken the enemy.

*“It’s worth mentioning that **Ukrainian leaders have turned to their own hackers for help** in the fight against Russia and this is precisely what they are doing. Ukrainian hackers and others worldwide are attacking infrastructures in Russia.”*

“Ukrainian leaders have turned to their own hackers for help in the fight against Russia and this is precisely what they are doing.”

The cybersecurity hub director told us that **the repercussions could be catastrophic if the hackers are successful and take aggressive measures** as the consequences of these cyberattacks would impact not just the countries involved, but the whole world.

He explained that the economies, foreign markets and, of course, supply chains of certain nations could be adversely affected.

width="900" loading="lazy">

Gonzalo García- Belenguer stressed the importance of developing cybersecurity tactics to control, manage, or eliminate these threats.

“Attacks on critical infrastructures ***could be life-threatening;*** *for example,* ***in the event of a malicious code causing an explosion at a nuclear power station.***

“Fortunately, this has not occurred; we hope that it stays that way and that ***this conflict will soon be over,****” he concluded.*

YOU’LL DEFINITELY WANT TO READ THIS TOO:

https://conecta.tec.mx/en/news/toluca/education/how-could-war-between-ukraine-and-russia-affect-your-cost-livin