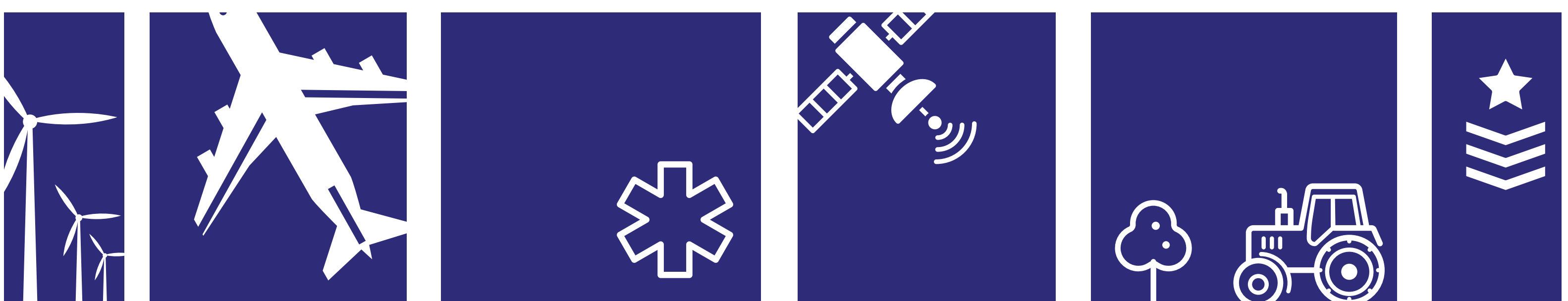


WHY CRITICAL NATIONAL INFRASTRUCTURE PROVIDERS NEED CYBER THREAT INTELLIGENCE

What is Critical National Infrastructure [CNI]?

Its key sectors include:



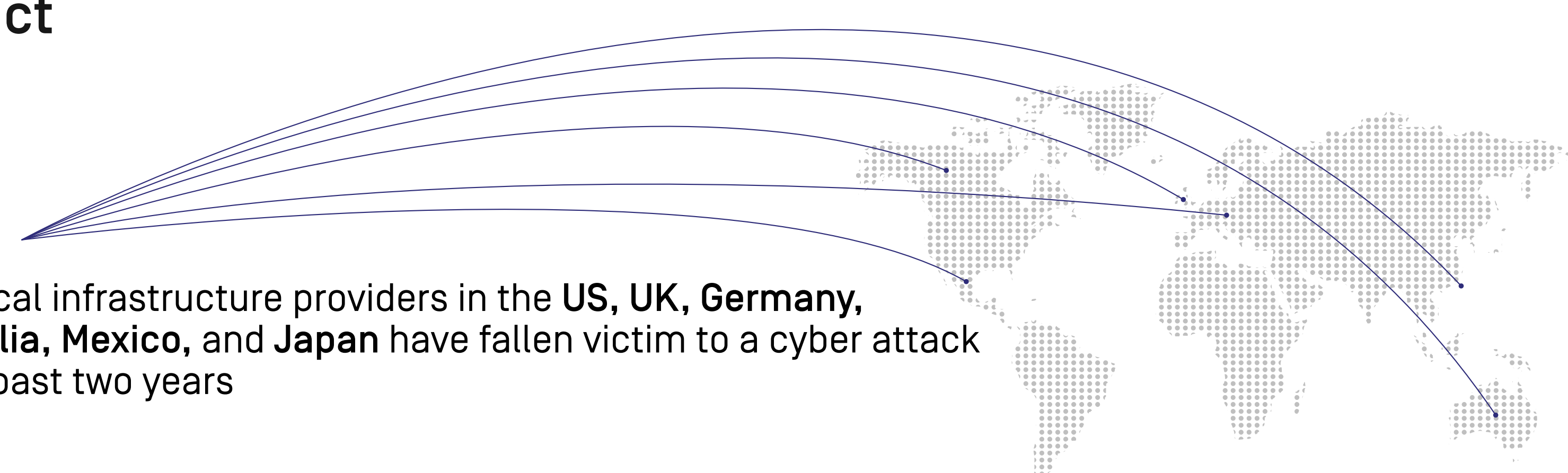
ENERGY TRANSPORTATION EMERGENCY SERVICES COMMUNICATIONS FOOD & AGRICULTURE DEFENSE^o

The risks



The impact

90% of critical infrastructure providers in the **US, UK, Germany, Australia, Mexico, and Japan** have fallen victim to a cyber attack in the past two years



Some recent high-profile attacks on CNI and their consequences:

2020 NTT Communications attack	621 corporate clients' data leaked ^o
2021 Colonial Pipeline attack	11,000 gas stations left without gas ^o
2021 JBS Foods attack	\$11 million ransom paid to hackers ^o

¹ <https://www.cisa.gov/critical-infrastructure-sectors>
² <https://www.bridewellconsulting.com/majority-of-cni-organisations-experience-successful-cyber-attacks-despite-strong-confidence-in-security>
³ <https://www.infosecurity-magazine.com/news/over-80-cni-firms-breached-past-36/>
⁴ <https://www.infosecurity-magazine.com/news/over-80-cni-firms-breached-past-36/>
⁵ <https://www.intelligentciso.com/2020/11/24/powering-up-cybersecurity-to-protect-cni/#>
⁶ <https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attacks-on-critical-infrastructure/>
⁷ <https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attacks-on-critical-infrastructure/>
⁸ <https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers>