NIGC Tech Alert

Shields UP! Russia's attack on Ukraine may have consequences for US Critical Infrastructure.

As suspected and planned for weeks, Russia has initiated an unprovoked attack on Ukraine. This attack has been accompanied by a multipronged and multifaceted series of cyber-attacks on Ukrainian government and business critical infrastructures. The response to these attacks from the US and our allies may have consequences for businesses and critical infrastructure here in the US, including tribal operations.

CISA (Cybersecurity And Infrastructure Security Agency) is highlighting this activity in their "Shields Up" awareness article and stated, "While *there are no specific or credible cyber threats to the U.S. homeland at this time*,… Every organization—large and small—*must be prepared to respond to disruptive cyber activity.*" To repeat, cyber-warfare poses stark risks to private businesses and government organizations alike, however reluctant they are to become participants or combatants. Escalating cyber conflict can lead to unanticipated consequences and casualties. No party is assured of remaining a mere spectator. Diligence and extra scrutiny and monitoring of critical systems and networks is highly recommended, especially in the coming days and weeks if indeed this cyber-war does escalate.

The assets of our tribal partners in Indian Country don't typically fall within the conventional definition of what one thinks of when "critical infrastructure" is mentioned such as electrical grids or water purification systems. This does NOT mean that tribal assets could not be affected by disruptions to other businesses, some more obviously critical, some less obvious. Be prepared for indirect attacks and disruptions or denial-of-service attacks on critical resources and vendors utilized by casinos and tribal entities to include but not limited to:

- Electrical, gas, and water utilities
- Traffic management
- Internet Service providers
- Cloud service providers
- Financial institutions
- Supply chain and logistics providers

The scope of the attacks and capabilities of nation-state threat actors are not limited to cyber attacks against critical infrastructure. Disinformation, misinformation, and social engineering attacks are ongoing and likely to increase in the coming days. Media literacy and mindfulness of phishing attempts are more critical than ever. Threat actors (Both state-sponsored and criminal syndicates) will take advantage of the anxiety, chaos, and also positive human emotions to commit acts of fraud. As an example, watch out for messages and websites from organizations claiming to be humanitarian charities.

For additional details and resources please visit:

CISA – Shield's Up < https://www.cisa.gov/shields-up>

CISA – Free Cybersecurity Services and Tools < https://www.cisa.gov/free-cybersecurity-services-and-tools>