The actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks. 

Rand Corp.

A type of warfare waged against government and military networks in order to disrupt, destroy, or deny their use.

Encyclopedia Britannica

Warfare consisting of attacks on computer systems of countries or institutions with the intention of disrupting, damaging, or destroying infrastructure.

Fortinet
State or non-state actors and their proxies, or criminal actors operating either at the behest of or with impunity within the sovereign territory of a nation-state, who engage in cyber-enabled malicious activities at or below the level of armed conflict with the strategic aim of inflicting harm to the government or private sectors of another nation.
DESTRUCTIVE CYBER ATTACKS

DATA THEFT & AGGREGATION

MALIGN INFLUENCE

CYBERCRIME

DATA THEFT & AGGREGATION

MALIGN INFLUENCE

CYBERCRIME

DESTRUCTIVE CYBER ATTACKS
DESTRUCTIVE CYBER ATTACKS
Actions by a nation-state resulting in effects similar to a kinetic attack: Stuxnet, NotPetya, WannaCry, Sony Pictures, OlympicDestroyer, Industroyer

MALIGN INFLUENCE
Hostile effort to influence public opinion or political, military, or economic policies through both overt and covert means

DATA THEFT & AGGREGATION
Collection of massive amounts of data through a combination of licit and illicit means to gain an information advantage

CRYPTOCURRENCY THEFT
Criminal actors operating in and through cyberspace at the direction or with the support of a nation-state: Conti, REvil, Killnet, XakNet

USA

Cyber Attacks

Malign Influence

Data Theft

01

02

03

04

Cyber Crime

Undersea Cables

Silicon Valley Venture Capital

Wikileaks

TikTok

Belt & Road Initiative

Fentanyl

Software Supply Chain

Ransomware

Decks

Belts

Cable

Belt

Undersea Cables

Wikileaks

TikTok

Silicon Valley Venture Capital

Fentanyl

C2SR

University IT

Second Annual Hybrid Cyber Security Research Symposium (CARS'22)
Social Media
Strengthen U.S. social media platforms, improve privacy, incentivize ethical and innovative uses of data; protect domestic space from adversary-controlled platforms

Private Sector
Zero-Trust for networks and communications, quantum-proof encryption modalities, responsible software development, immediate patching, data obfuscation

Government
Department of Digital Services, U.S. Cyber Force, updates to international law, increase access to high-speed internet

Partnership
Threat intelligence sharing, marketplace, incentivize bottom line, incentivize innovation
QUESTIONS AND DISCUSSION

Michael G. McLaughlin
Cybersecurity Attorney | Policy Advisor
MGMcLaughlin@BakerDonelson.com