Threat Actor Comparision Matrix

	APT / Group	Characteristics	Technical Capabilities and Preferred TTPs	Historical Targeting Patterns	Capability (0–5)	Motive Alignment (0–5)	Infrastructure Overlap (0–5)	Total	Confidence Level	Notes
1	Sandworm (GRU-linked)	Russian state-sponsored destructive threat group attributed to GRU Unit 74455; focused on sabotage of critical infrastructure.	Custom ICS malware (e.g., Industroyer, BlackEnergy); high sophistication in protocol exploitation; TTPs: Spearphishing Attachment (T1566.001), Data Destruction (T1485), Firmware Corruption (T1495).	Ukrainian energy sector (2015-2016 power grid attacks), global via NotPetya (2017), French Olympics (2018), Georgian infrastructure. Targets governments, energy, and military in conflict zones.	5	5	4	14	High	Known ICS disruption (Ukraine, NotPetya), destructive tooling
2	APT28 (Fancy Bear)	Russian GRU-linked cyber espionage group; known for political interference and intel gathering.	Custom ICS malware (e.g., Industroyer, BlackEnergy); high sophistication in protocol exploitation; TTPs: Spearphishing Attachment (T1566.001), Data Destruction (T1485), Firmware Corruption (T1495).	NATO countries, Eastern Europe governments (e.g., German Bundestag 2015), US DNC (2016), WADA, military entities. Focus on espionage during elections and conflicts.	4	3	3	10	Medium	Espionage focus, but capable of disruptive ops
3	APT29 (Cozy Bear)	Russian SVR-linked stealthy espionage group; long-term access specialists.	Custom ICS malware (e.g., Industroyer, BlackEnergy); high sophistication in protocol exploitation; TTPs: Spearphishing Attachment (T1566.001), Data Destruction (T1485), Firmware Corruption (T1495).	US DNC (2016), US State Dept, global via SolarWinds (2020), political parties, tech firms. Targets governments and tech for intel.	3	3	2	8	Low–Medium	Stealthy espionage, limited ICS precedent
4	Lazarus Group	North Korean state-sponsored; mix of espionage, destruction, and financial crime.	Custom ICS malware (e.g., Industroyer, BlackEnergy); high sophistication in protocol exploitation; TTPs: Spearphishing Attachment (T1566.001), Data Destruction (T1485), Firmware Corruption (T1495).	Sony Pictures (2014), Bangladesh Bank (2016), WannaCry global (2017), crypto exchanges, governments in South Korea and US. Targets financial and media for profit and disruption.	4	4	2	10	Medium	DPRK-linked, destructive capacity, mixed motives
5	Revil / DarkSide	Russian-speaking criminal ransomware groups; RaaS model with affiliates.	Ransomware variants; double extortion; TTPs: Exploit Remote Services (T1210), Supply Chain Compromise (T1195), Data Encrypted for Impact (T1486).	Colonial Pipeline (DarkSide, 2021), Kaseya supply chain (REvil, 2021), global enterprises in energy and IT. Targets large corporations for financial gain.	3	4	3	10	Medium	Ransomware groups, supply-chain proven (Kaseya)
6	APT40 (Leviathan)	Chinese MSS Hainan-linked espionage group; focus on maritime and regional intel.	Custom RATs; phishing kits; TTPs: Spearphishing Link (T1566.002), Command and Control via Web Protocols (T1071.001), Exfiltration Over Web Service (T1567).	Asia-Pacific governments, shipping firms, universities (e.g., South China Sea disputes); biomedical and defense sectors since 2014.	3	3	2	8	Low–Medium	Maritime & industrial espionage, less ICS history
7	Turla (Snake/Uroburos)	Russian FSB-linked advanced espionage group; known for long-term persistence.	Rootkits and Snake implant; TTPs: Boot or Logon Initialization Scripts (T1037), Valid Accounts (T1078), Remote Services (T1021).	US DoD, European governments, diplomatic entities since 2004; targets military and intel agencies.	4	3	3	10	Medium	Russian-linked, advanced persistence & stealth
8	Charming Kitten (APT35)	Iranian IRGC-linked cyber espionage; social engineering experts.	Phishing sites, custom malware (e.g., PowerLess); TTPs: Spearphishing Attachment (T1566.001), Social Engineering (T1566), Credential Access (TA0006).	Middle East dissidents, US/Europe governments, COVID vaccine orgs (2020), Israeli entities. Targets political opponents and intel.	2	2	1	5	Low	Iranian espionage, limited ICS capacity
9	OilRig (APT34)	Iranian MSS-linked; targets energy and regional governments.	Custom tools (e.g., DNSpionage); TTPs: DNS Hijacking (T1556.004), Web Shell (T1505.003), Supply Chain Compromise (T1195).	Middle East energy sector, governments (e.g., Saudi Arabia, Israel); telecom and finance since 2014.	3	3	2	8	Low–Medium	Iranian, regional targeting, some OT focus
10	Hafnium	Chinese state-sponsored; vulnerability exploitation focus.	Zero-day exploits (e.g., Microsoft Exchange); TTPs: Exploit Public-Facing Application (T1190), Web Shell (T1505.003), External Remote Services (T1133).	Microsoft Exchange servers globally (2021), tech and government entities in US/Europe. Targets for espionage and data theft.	3	3	2	8	Low–Medium	Chinese state-linked, Exchange exploits, less ICS focus
11	Mustang Panda	Chinese-sponsored espionage; uses regional lures (e.g., Mongolian-themed).	PlugX RAT; TTPs: Spearphishing Attachment (T1566.001), Supply Chain Compromise (T1195), Command and Control (TA0011).	Asia-Pacific governments, NGOs, minorities (e.g., Myanmar, Southeast Asia); public and private sectors since 2017.	3	3	1	7	Low	Chinese, politically targeted espionage
12	Unknown / False Flag Actor	Deliberate misdirection using mimicked artifacts; variable affiliation.	Shared/open-source tools; planted indicators; TTPs: Mimic other groups' TTPs (e.g., false linguistic clues), Obfuscated Files (T1027).	Historical examples: Olympic Destroyer (2018) mimicking Lazarus but attributed to Sandworm; various nation-state ops to shift blame. Targets depend on true actor.	2	5	1	8	Variable	May be deliberate misdirection using open-source tools