FIGURE 4.1
Operational Capacity Definitions

OC1 Amateur attempts

Operations roughly less capable than or comparable to a single individual with some limited professional expertise in information security spending several days with a total budget of up to $1,000 on the specific operation, and no preexisting infrastructure or access to the organization.

This includes the operations of many **hobbyist hackers**, as well as more experienced hackers who implement completely untargeted **"spray and pray" attacks.**

OC2 Professional opportunistic efforts

Operations roughly less capable than or comparable to a single individual who is broadly capable in information security spending several weeks with a total budget of up to $10,000 on the specific operation, with preexisting personal cyber infrastructure but no preexisting access to the organization.

This includes the operations of many **individual professional hackers**, as well as **capable hacker groups when executing untargeted or lower-priority attacks.**

OC3 Cybercrime syndicates and insider threats

Operations roughly less capable than or comparable to ten individuals who are experienced professionals in information security spending several months with a total budget of up to $1 million on the specific operation, with major preexisting cyberattack infrastructure but no preexisting access to the organization. Also included in this category are attempts by insider threats within the organization, who will have significantly less resources and expertise than the previous operations described as part of this category but significant access to sensitive organization resources (e.g., a senior member of the organization's research team).

This includes the operations of many **world-renowned criminal hacker groups**, **well-resourced terrorist organizations**, **disgruntled employees**, and **industrial espionage organizations.**[a]

OC4 Standard operations by leading cyber-capable institutions

Operations roughly less capable than or comparable to 100 individuals who have experience in a variety of relevant professions (cybersecurity, human intelligence gathering, physical operations, etc.) spending a year with a total budget of up to $10 million on the specific operation, with vast infrastructure and access to state resources such as legal cover, interception of communication infrastructure, and more.

This includes the operations of many of the world's leading **state-sponsored groups** and many **foreign intelligence agencies** across the world. The top cyber-capable nations globally can execute such operations more than **100 times per year.**

OC5 Top-priority operations by the top cyber-capable institutions

Operations roughly less capable than or comparable to 1,000 individuals who have experience and expertise years ahead of the (public) state of the art in a variety of relevant professions (cybersecurity, human intelligence gathering, physical operations, etc.) spending years with a total budget of up to $1 billion on the specific operation, with state-level infrastructure and access developed over decades and access to state resources such as legal cover, interception of communication infrastructure, and more.

This includes the handful of operations most prioritized by the world's **most capable nation-states.**

[a] The set of actors within OC3 is more diverse than in other categories—most notably in the inclusion of both insider threats and external cyber organizations. We group the OC3 actors together because the level of investment required to robustly defend against them is comparable, despite the specific measures required being partially but not fully overlapping.