Źródła zagrożeń różnią się pod względem możliwości podmiotów, ich gotowości do działania oraz motywów, którymi się kierują, łącznie z korzyściami finansowymi. Potencjalnie podmioty będące źródłem cyberzagrożeń posługują się różnymi technikami ataków na sieci i systemy teleinformatyczne oraz ich elementy czy zasoby. Są w stanie przechwytywać lub wykradać wartościowe dane i informacje. Rozmiar zagrożenia zależy od złożoności, skomplikowania sposobu przeprowadzenia cyberataku. Cyberataki mogą być kombinacją wielu różnych technik. Za ich pomocą potencjalnie zagrażające podmioty mogą podejmować działania zarówno przeciwko celom pojedynczym, np. komputery osobiste lub stacje robocze, jak i zbiorowym, np. sieci i systemy teleinformatyczne sił zbrojnych.

Kategorie te nie wykluczają się wzajemnie. Na przykład działania pojmowane przez jeden podmiot jako hacktivism mogą być pojmowane przez inny podmiot jako cyberterroryzm. Klasyfikacja przedstawiona w tabeli 2.1. ma na celu zidentyfikowanie głównych rodzajów istniejących zagrożeń w celu określenia najbardziej odpowiedniego i skutecznego podejścia do zakresu ryzyka, jakie stwarzają.

Pozostające w obszarze odpowiedzialności sił zbrojnych obiekty funkcjonujące z wykorzystaniem sieci lub systemów teleinformatycznych, same sieci i systemy teleinformatyczne, ich zasoby, a także żołnierze mogą być atakowani nie tylko przez napastników państwowych, ale również przez podmioty niepaństwowe. Różni atakujący będą skupiać się na różnych celach, posiadać różne motywacje i stosować różne metody ataku. W tabeli 2.2. przedstawiono punkt widzenia Johana Sigholma na temat podziału niepaństwowych podmiotów prowadzących cyberdziałania.

TABELA 2.2. Główni niepaństwowi cybernapastnicy

Napastnik	Motywacja	Cel	Metoda
Zwykli obywatele	Brak (słaba)	Żaden	Pośrednia
Script kiddies	Ciekawość, dreszczyk emocji, ego	Osoby indywidualne, firmy, rządy	Wcześniej napisane skrypty i narzędzia
Haktywiści	Zmiany polityczne lub społeczne	Osoby decyzyjne lub przypadkowe ofiary	Protesty poprzez wandalizm witrynowy lub ataki DDoS
Hakerzy black-hat	Ego, osobiste porachunki, korzyści ekonomiczne	Żaden	Oprogramowanie złośliwe
Hakerzy white-hat (ethical hackers)	Idealizm, kreatywność, szacunek dla prawa	Żaden	Testy penetracyjne, łatanie