3

TEORETYCZNE PODSTAWY CYBERWALKI

W literaturze przedmiotu istnieje pogląd, że *cyberdziałania* to zbiór przeważnie nielegalnych działań w cyberprzestrzeni, prowadzonych przez podmioty niepaństwowe, powodujące szkody lub zakłócenia w dążeniu do różnych celów politycznych, ekonomicznych lub osobistych[1]. Definicja ta określa jakoby cyberdziałania były realizowane jedynie przez podmioty niepaństwowe. Uwypukla także jej nielegalność. Ten punkt widzenia wydaje się dyskusyjny, ponieważ siły zbrojne są podmiotem państwowym, który cyberdziałania prowadzi. A działania takie w określonych warunkach (np. w czasie wojny) mogą być w myśl zasady *ius in bello* legalne.

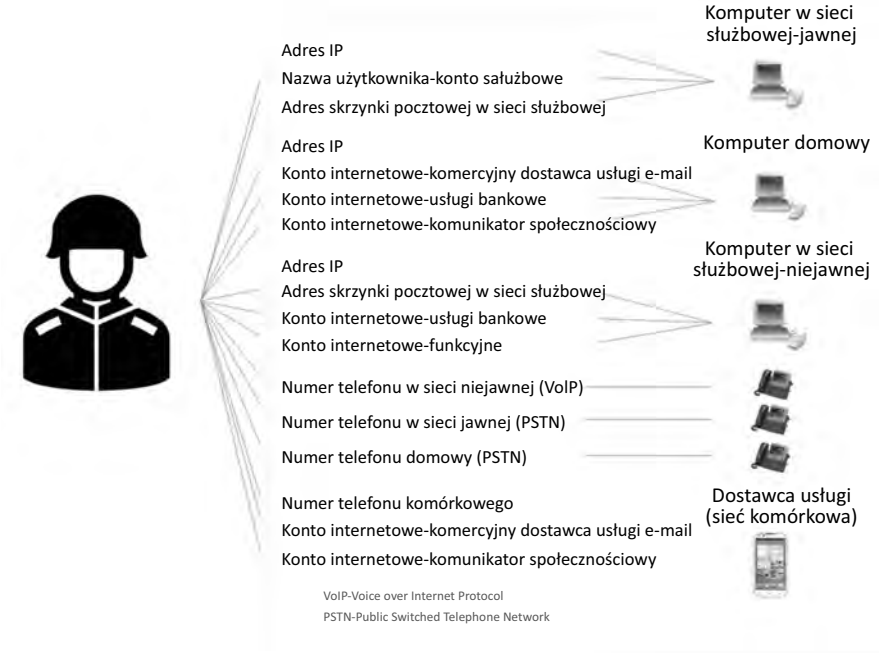
Cyberdziałania mogą być prowadzone szeregowo albo równolegle razem z bezpośrednimi działaniami konwencjonalnymi. W pierwszym przypadku poprzedzają je lub prowadzone są po ich zakończeniu, w drugim konwencjonalne działania bezpośrednie prowadzone są jednocześnie (z różną intensywnością) z tymi w cyberprzestrzeni. W przypadku gdy cyberwalka prowadzona jest w ramach połączonej operacji wojskowej, cyberdziałania powinny być integralną częścią działań wojsk. Wówczas świadomość sytuacyjna w cyberprzestrzeni dowodzących cyberdziałaniami powinna być częścią całkowitej świadomości sytuacyjnej dowódców prowadzących operacje wojskowe.

[1] J. Sigholm, *Non-State Actors in Cyberspace Operations*, Journal of Military Studies, 4(1)\2013, s. 6.

Gdy cyberwalka prowadzona jest jedynie przez cyberwojska w ramach np. cyberoperacji, świadomość sytuacyjna w cyberprzestrzeni dowodzących cyberdziałaniami będzie obejmować jedynie zagadnienia związane z cyberdziałaniami.

Wśród wojskowych istnieje opinia, iż cyberdziałania powinny prowadzić wyłącznie wojska właściwe do cyberwalki. Mając na uwadze wąską specjalizację takich sił oraz specyfikę przestrzeni prowadzenia cyberwalki, pogląd ten może wydawać się słuszny. Jednak rozproszenie współczesnej przestrzeni walki oraz możliwości oddziaływania przeciwnika na zasoby teleinformatyczne wojsk wymuszają, aby niektóre zadania z zakresu cyberwalki prowadzili żołnierze wszystkich rodzajów wojsk i sił zbrojnych.

Indywidualnym środkiem walki żołnierza jest jego broń osobista. Każdy walczący żołnierz posiada broń i zdolność do korzystania z niej. Żołnierze przygotowani są do realizacji zadań i czynności w zakresie wielu specjalizacji, od medycznej poprzez inżynieryjną aż po ochronę chemiczną. Również każdy żołnierz prowadzący walkę (bez wyjątku) jest bezpośrednio lub pośrednio związany z różnymi sieciami lub systemami teleinformatycznymi (rysunek 3.1.) lub może być także wyposażony w urządzenia wykorzystujące informatykę, stanowiące część osobistego ekwipunku. To powoduje, że umiejętne posługiwanie się teleinformatyką lub dostarczanymi za jej pośrednictwem usługami może być



RYSUNEK 3.1.
Zależność żołnierza od sieci i systemów teleinformatycznych

Źródło: Opracowanie własne.