GEERS, KENNETH. STRATEGIC CYBER SECURITY

JAKUB HARAŠTA

GEERS, Kenneth. *Strategic Cyber Security*. Tallinn: CCD COE Publication, 2011, 169 s. ISBN 9789949904075 (pdf).

V souvislosti s rozvojem informační společnosti jsou otázky kybernetické společnosti vnímány jako důležité soukromými společnostmi, vládami i mezinárodními organizacemi. Po zkušenostech z roku 2007, kdy se cílem rozsáhlého kybernetického útoku stalo Estonsko, vzniklo pod hlavičkou NATO v Tallinnu Centrum excelence kybernetické bezpečnosti (CCD COE). Jednou z publikací představených tímto pracovištěm je recenzovaná publikace z pera zástupce USA při CCD COE.

Geers konstatuje, že se kybernetická bezpečnost vyvinula z pouhé technické disciplíny ve strategický koncept[1], k němuž musejí zodpovědně přistupovat celé národy, pokud si mají zachovat svůj životní standard v současném světě. Ve své knize se věnuje konceptualizaci strategie (kap. II[2]), popisu čtyř různých národních strategií použitelných pro zmenšení rizika kybernetických útoků (kap. III[3]) a závěrům o vhodnosti použití těchto strategií za užití metody DEMATEL (kap. IV[4]).

V těžišti knihy, kterou je kapitola III, zahrnují rozebírané strategie škálu opatření od čistě technických (implementace protokolu IPv6), přes vojenská (aplikace historicky nejúspěšnější vojenské doktríny založené na Umění války od Sun Tzu) až po hybridně politické (odstrašování[5] jako vojensko-politický koncept a kontrola kybernetických zbraní jako koncept politicko-technický). Protokol IPv6 je často vnímán jako zásadní technický krok

[1] GEERS, Kenneth. Strategic Cyber Security. Tallinn: CCD COE Publication, 2011, 169 s. ISBN 9789949904075 (pdf). S. 5

[2] Ibid., s. 19-86.

[3] Ibid., s. 87-131.

[4] Ibid., s. 132-154.

[5] Angl. deterrence.

vstříc lepšímu zajištění bezpečnosti (a stejně tak je Geersem i popisován[6]) a zároveň se jeví jako nezbytnost v souvislosti s narůstajícím množstvím zařízení připojených k internetu. IPv6 je obecně vstřícnější k užívání kryptografie, dále umožňuje vzhledem k téměř neomezenému množství IP adres end-to-end spojení a je logičtější (vzhledem k alokaci adres nebo směrování paketů). Na druhé straně se ale již v minulosti ukázalo, že IPv6 jako takový není bezpečný ani před typickými dnešními útoky (DOS a MitM útoky). Geersovým závěrem je, že implementace IPv6 by měla (při implementaci všech čtyř v knize představených strategií) největší vliv na zvýšení míry kybernetické bezpečnosti.[7] Ze tří zbylých strategií by měla největší vliv implementace vojenské doktríny inspirované Uměním války od Sun Tzu, kterou vnímá jako dostatečně flexibilní i pro aplikaci v prostředí kybernetického boje. V této části se Geers poměrně překvapivě odklání od samotné aplikace této vojenské doktríny, ale uzavírá myšlenku popisem deseti specifik kybernetického bojiště, které by aplikaci mohly optikou současných vojenských struktur znemožnit.[8]

Ve svých závěrech přikládá Geers zbylým dvěma řešením spíše marginální význam, přestože jim je jinak věnována značná politická pozornost. Představená strategie odstrašování[9] navazuje na odstrašování nukleárními zbraněmi jako hlavní metodu udržování rovnováhy v průběhu Studené války. Geers sice odmítá srovnávat následky nukleárního výbuchu s kybernetickým útokem, nepodceňuje však vliv cíleného kybernetického útoku na moderní společnost. V rámci kontroly kybernetických zbraní Geers opakovaně upozorňuje na terminologické a navazující praktické problémy[10] a také na nedostatek politické vůle k přijetí mezinárodní úmluvy, která by tuto oblast regulovala.

Kniha jako celek představuje zajímavý příspěvek do diskuze o konkrétních aspektech strategické kybernetické bezpečnosti a vzhledem k rozsáhlé bibliografii se dá použít i jako základní literatura pro pochopení různých přístupů k regulaci kybernetické bezpečnosti.

---

[6] I když zmiňuje i obavy z vlivu IPv6 na soukromí na internetu. Ibid., s. 87.

[7] Ibid., s. 152.

[8] Ibid., s. 110.

[9] Geersem rozdělená na odepření přístupu (např. skrze legislativu zaměřenou na technologie dvojího užití) a potrestání (např. preemptivní údery, sankce).

[10] Jen těžko lze provádět inspekce směřující k nalezení kybernetické zbraně za předpokladu, že pojem kybernetické zbraně jako takové není předmětem konsensu.