Journal of KONBiN 2020
Volume 50, Issue 4
DOI 10.2478/jok-2020-0089

Sławomir DYGNATOWSKI
Military University of Aviation (Lotnicza Akademia Wojskowa)

CYBERBEZPIECZEŃSTWO JAKO FUNDAMENT BEZPIECZEŃSTWA INFRASTRUKTURY KRYTYCZNEJ W KONTEKŚCIE WSPÓŁCZESNYCH ZAGROŻEŃ

Cyber security as a foundation for the security of critical infrastructure in the context of modern threats

Streszczenie: *Artykuł ma na celu przedstawienie zarysu najbardziej charakterystycznych cech problemu wzrostu roli i przewagi cyberbezpieczeństwa jako kluczowego elementu funkcjonowania infrastruktury krytycznej i możliwości jego rozwiązania. Z uwagi na fakt, że ze wszystkich systemów obejmujących infrastrukturę krytyczną najważniejszy dla właściwego funkcjonowania gospodarki i społeczeństwa jest system zaopatrzenia w energię, surowce energetyczne i paliwa, w artykule poddano analizie przeszły, teraźniejszy oraz przyszły stan zagrożeń i ewolucji narzędzi do ich zwalczania. Szczególny nacisk położono na charakterystykę tych zagrożeń, w tym przede wszystkim cyberataków, jak również najefektywniejsze sposoby ich zwalczania. Artykuł wpisuje się w debatę o kluczowym wpływie cyberataków na infrastrukturę krytyczną, co ma bezpośredni wpływ na bezpieczeństwo narodowe.*
Słowa kluczowe: cyberbezpieczeństwo, infrastruktura krytyczna

Abstract: *The article's goal is to outline the most characteristic features of the problem of the growing role and predominance of cybersecurity as a key element in the functioning of critical infrastructure and the possibilities of the best solutions. Due to the fact that from all systems of critical infrastructure, the most important for the proper functioning of the economy and society is the system of energy and fuel supply. The article will analyze past, present and future threats and evolution of tools to combat them. Particular emphasis will be placed on the characteristics of these threats, especially cyberattacks, as well as the most effective ways of counter-actions. The article might be an element of the debate on the critical impact of cyberattacks on critical infrastructure, which has a direct impact on national security.*
Keywords: cybersecurity, critical infrastructure

1. Wprowadzenie

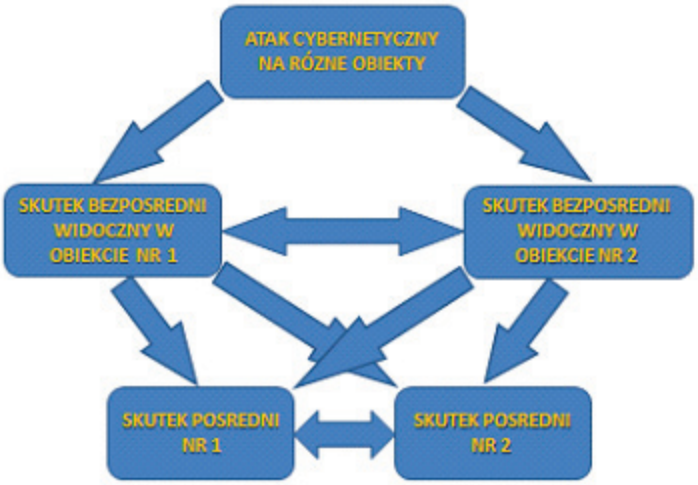
Wzrost roli i wagi cyberbezpieczeństwa jako kluczowego elementu funkcjonowania infrastruktury krytycznej staje się globalnym trendem. Nowe wyzwania, aby zapewnić bezpieczeństwo w tym strategicznym obszarze każdego państwa, wynikają z uzależnienia od technologii informacyjno-komunikacyjnych jako priorytetowych wśród innych rodzajów ochrony infrastruktury krytycznej, tj. ochrony fizycznej, technicznej, osobowej i prawnej. Infrastruktura krytyczna podlega ciągłym zmianom, które wynikają z rozwoju cywilizacyjnego człowieka oraz, jednocześnie, stają się podatne na zagrożenia, które będą adekwatne wobec tempa i kierunku tego rozwoju.

2. Analiza problemu

Ze wszystkich systemów obejmujących infrastrukturę krytyczną, najważniejszy do właściwego funkcjonowania gospodarki i społeczeństwa jest system zaopatrzenia w energię, surowce energetyczne i paliwa. Bez energii, w szczególności bez regularnych dostaw surowców energetycznych i paliw, żaden inny element infrastruktury krytycznej nie może działać. Było to szczególnie widoczne w działaniach rządu USA po przejściu przez Stany Zjednoczone huraganu Sandy w 2012 r., który jako priorytet wyznaczył sobie przywrócenie energii elektrycznej, a następnie systemu transportowego (autobusy i metro). Z drugiej strony, w niektórych przypadkach nie potrzeba katastrof naturalnych, aby sparaliżować jeden z elementów systemu. W 2003 r. we Włoszech kontakt przewodów elektroenergetycznych z gałęziami drzewa spowodował awarię, w efekcie której cały tranzyt energii skierowany został na inną linię, która po przeciążeniu uległa automatycznemu wyłączeniu. W wyniku efektu domina doszło do całkowitej izolacji włoskiego systemu elektroenergetycznego od sieci na granicach: francusko-włoskiej, szwajcarsko-włoskiej, słoweńsko-włoskiej i austriacko-włoskiej. To spowodowało tzw. blackout, który trwał ok. 9 godzin i dotknął ponad 50 milionów ludzi w samych Włoszech, w tym m.in. pasażerów 110 pociągów, pacjentów szpitali, a także lotniska, które mimo posiadania awaryjnych źródeł zasilania, zostały sparaliżowane z powodu braku prądu [1]. O ile człowiek nie ma wpływu na występowanie zagrożeń naturalnych, o tyle może próbować minimalizować zagrożenia terrorystyczne i techniczne [13].

Mamy w tym przypadku do czynienia ze skutkami bezpośrednimi, które zazwyczaj pojawiają się natychmiast i które można łatwo rozpoznać. W przeciwieństwie do nich, skutki pośrednie kreowane są poprzez mechanizmy lub efekty pośredniczące pomiędzy działaniem pierwotnym (inicjującym) a fizycznym lub psychologicznym skutkiem finalnym. Skutki te zazwyczaj ujawniają się z opóźnieniem i mogą być trudne do ustalenia [16]. Dość łatwo można dostrzec zależności pomiędzy skutkami pośrednimi i bezpośrednimi. Przykładem jest cybernetyczny atak na rafinerię ropy naftowej. Zniszczenie jednej rafinerii wywoła skutek bezpośredni w postaci wyłączenia jej z pracy. Jednakże, gdy

zniszczonych lub obezwładnionych zostanie kilka rafinerii, możemy doświadczyć skutków pośrednich, np. w postaci unieruchomienia transportu w całym kraju z powodu braku paliwa. Rezultat ten pojawi się natychmiast. Musi upłynąć pewien czas, kiedy wszelkie zależne podmioty będą korzystały ze zgromadzonych zapasów. W tym okresie trudno rozpoznać skutki pośrednie, jakie spowodowało zniszczenie tych rafinerii, lecz wraz z upływem czasu będą one narastały lawinowo.



Rys. 1. Interakcje pomiędzy skutkami pośrednimi i bezpośrednimi [na podst. T.W. Beagle Jr, Effects-Based Targeting: Another Empty Promise?]

Największy problem polega jednak na tym, że terroryści, ekstremalni protestujący lub tzw. haktywiści (pot. hakerzy działający z pobudek społecznych), doskonale wiedzą, że odporność systemów o krytycznym znaczeniu dla państwa jest tak dobra, jak ich najsłabszy punkt. Terroryzm stanowi trzecią i ostatnią kategorię zagrożeń, które mogą wywołać sytuację kryzysową mającą wpływ na bezpieczeństwo i funkcjonowanie całego państwa lub jego poszczególnych regionów [13]. Wspomniani ekstremalni protestujący mogą swoimi działaniami wywoływać skutki tak samo katastrofalne jak te wywołane przez atak terrorystyczny, dlatego też nie można ich pomijać w dyskusji na temat elementów składowych zagrożeń terrorystycznych dla infrastruktury krytycznej. W celu ochrony instalacji i zapewnienia bezpieczeństwa pracowników platformy i samych protestujących, duńska policja w 2011 r. musiała usunąć aktywistów organizacji Greenpeace, protestujących na platformie wiertniczej Leiv Eiriksson, jednej z największych i najnowocześniejszych na świecie [5].

Znanym w historii, celowym atakiem na strukturę energetyczną, który stanowił niezbędny element strategii działań wojennych, była operacja „Chastise" z maja 1943 r. Była to jedna z najbardziej brawurowych akcji II wojny światowej, mająca na celu zniszczenie przez siły lotnicze Wielkiej Brytanii zapór na rzekach w Zagłębiu Ruhry,

mających krytyczne znaczenie dla niemieckiej infrastruktury energetycznej [4]. Z samej operacji można wysnuć dwa interesujące wnioski, wciąż aktualne w obecnych czasach i w obliczu nowych zagrożeń i wyzwań. Po pierwsze, ataki na infrastrukturę krytyczną wymagały rozwiązań innowacyjnych i wysoce oryginalnych. Brytyjski inżynier lotnictwa Barnes Wallis nie tylko wynalazł i skonstruował nowy rodzaj uzbrojenia, tzw. skaczące bomby, ale także opracował koncepcję ataku newralgicznych elektrowni i zapór wodnych jeszcze przed II wojną światową, twierdząc, że duże cele przemysłowe powinny być wyłączone z listy celów bombardowań strategicznych na rzecz elektrowni, infrastruktury kolejowej, a w szczególności mostów. Faktycznie, z uwagi na specyficzną metodę zrzutu na cel „skaczące bomby" były wyjątkowe i bez większych przeszkód przerwały zapory Mohne i Eder, zbudowane ze zbrojonego betonu[1]. Jednak zapora Sorpe, której wnętrze tworzyły masy zbitej ziemi, okazała się odporna na bombardowanie i została jedynie nieznacznie naruszona. Drugim wnioskiem płynącym z operacji „Chastise" jest zatem konieczność wdrażania odpowiedniego sposobu budowania i konstruowania obiektów infrastruktury krytycznej. 75 lat po tych wydarzeniach to właśnie innowacja i odporność stanowią dwie kluczowe cech, od których zależy skuteczność ochrony infrastruktury krytycznej, również w odniesieniu do ataków cybernetycznych, które zaczęły przypominać w swoich efektach bezpośrednie działania grup terrorystycznych na systemy infrastruktury krytycznej.

Niedoszły atak Irlandzkiej Armii Republikańskiej w 1996 r. na cztery stacje elektroenergetyczne, zapewniające prąd Londynowi, miał zachwiać gospodarką Wielkiej Brytanii na wiele miesięcy [19]. Pokazało to ogromną podatność infrastruktury krytycznej na bezpośrednie działania terrorystyczne. To samo dotyczy również wyłączania lub niszczenia poszczególnych elementów systemu skomplikowanej sieci powiązań. Wywołanie globalnej paniki przez terrorystów nakładem minimalnych kosztów pokazują wydarzenia z 2002 r., kiedy Al-Kaida zaatakowała francuski tankowiec Limburg niewielką łodzią rybacką wyładowaną 200 kg trotylu. Choć zginęła tylko jedna osoba, a straty materialne były niewielkie, giełda zareagowała na atak histerycznie [21]. W kontekście współczesnych, regularnych ataków bliskowschodnich grup terrorystycznych na infrastrukturę energetyczną, np. udaremniony atak terrorystów z Państwa Islamskiego na rafinerię Baiji w Iraku w 2015 r. [3], należy pamiętać, że jakikolwiek udany zamach na świecie powoduje regionalną reakcję łańcuchową i z czasem wpływa pośrednio na wszystkie państwa. W perspektywie globalnego wydobycia ropy naftowej wielkości ok. 90 milionów baryłek

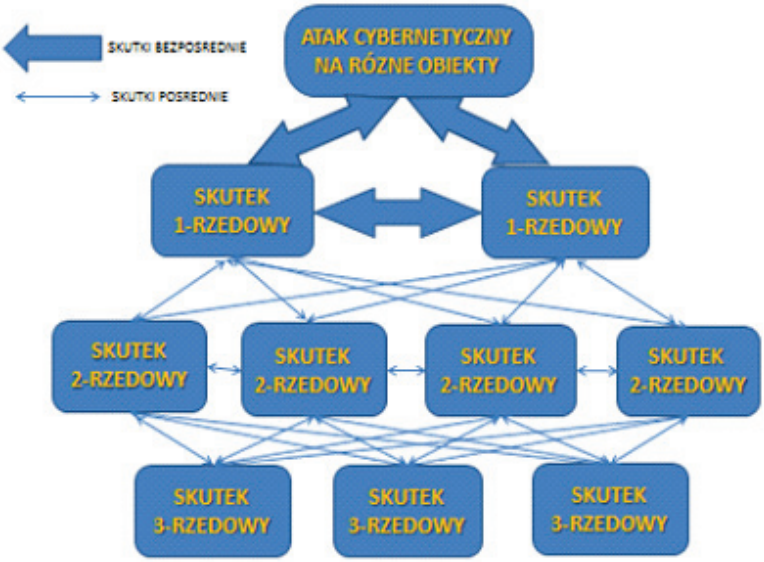
[1] Samolot musiał lecieć z prędkością od 230 do 235 mil na godzinę (około 370 km/h) na wysokości około 60 stóp (20 m) nad powierzchnią wody i zrzucić bombę tak, aby uderzając o płaszczyznę wody odbiła się od niej i zachowując energię kinetyczną „podskakiwała" (jak „kaczka" z kamienia) kilkakrotnie (na długości ok. 400 m), aż do osiągnięcia celu, którym były korony zapory wodnej. Przed zrzutem bomby używano specjalnego urządzenia, które wprowadzało bombę w ruch obrotowy. Dzięki temu bomba łatwiej odbijała się od powierzchni, nie tonąc po zetknięciu z nią. Po dotarciu do zapory, bomba tonęła i na głębokości ok. 30 stóp (ok. 10 m) dochodziło do eksplozji, https://pl.wikipedia.org/wiki/Bomba_skacz%C4%85ca (dostęp 17 listopada 2018 r.).

dziennie i takiego samego dziennego zużycia, każde naruszenie tej proporcji, nawet na poziomie 2% oznacza znaczące konsekwencje dla cen ropy oraz światowej gospodarki. W przypadku realnego incydentu wyłącznie Arabia Saudyjska jest w stanie szybko nadrobić deficyt w zasobach [9]. Ataki cybernetyczne na infrastrukturę krytyczną są tak samo tragiczne w skutkach jak fizyczne ataki terrorystyczne, a przy tym wymagają minimalnych zasobów ludzkich i kapitałowych oraz pozbawione są barier lokalizacyjnych.

Łatwo zauważyć, że organizacje terrorystyczne lub państwa planujące atak cybernetyczny na infrastrukturę krytyczną przeciwnika zyskują na wykorzystaniu broni cyfrowych, które oprócz zniszczenia lub obezwładnienia celu pierwszoplanowego spowoduje osiągnięcie pożądanych skutków politycznych i wojskowych. Siły zaangażowane w cyberatak w dalszym ciągu będą oddziaływać na obiekty przeciwnika, lecz ich zniszczenie jest tylko jednym ze skutków mieszczącym się w zbiorze pożądanych przez atakującego opcji prowadzonych działań. Najczęściej będzie ono pierwszym krokiem na drodze ku kolejnym, wynikającym z wyższych efektów oczekiwanego porażenia. Takie twierdzenie mieści się w koncepcji targetingu o złożonych skutkach, w której to teorii postrzega się zniszczenie lub porażenie obiektu w nakazanym stopniu przede wszystkim jako środek do osiągnięcia innych efektów, a nie jako skutek końcowy. Istota takiej operacji cybernetycznej o złożonych skutkach zasadza się na wykorzystaniu efektu zniszczenia (lub innego uzyskanego za pomocą broni nieniszczącej) do wygenerowania ustalonego z góry efektu drugorzędowego, który z kolei skłoni decydentów przeciwnika do reakcji pomyślnej dla sformułowanych przez atakującego ogólnych celów jego kampanii. Spleciona w ten sposób sieć efektów pozwala oczekiwać, że siły działające w cyberprzestrzeni mogą być użyte w sposób ekonomiczny, ściślej wiążąc osiągane rezultaty z założonymi celami działania, co jest niezwykle ważne w czasach finansowych i materiałowych ograniczeń współcześnie prowadzonych działań.

Przełom w postrzeganiu chociażby przez Sojusz Północnoatlantycki bezpieczeństwa energetycznego i kolektywna deklaracja jego zaangażowania w ten obszar nastąpiły dopiero podczas szczytu Sojuszu w Rydze w 2006 r. Pomimo że agendy sojusznicze uwzględniają obecnie zabezpieczenie dostaw energii, utrzymywanie bezpieczeństwa szlaków przesyłowych oraz rozwój kompetencji NATO w ochronie infrastruktury energetycznej, samą realizację polityki bezpieczeństwa energetycznego (i jej podstawowych elementów, w tym m.in. dywersyfikację źródeł energii czy bezpieczeństwo dostaw) Sojusz pozostawia bezpośrednio w gestii państw członkowskich i wyspecjalizowanych agend międzynarodowych. Dalszemu rozwojowi aktywności Sojuszu na polu bezpieczeństwa energetycznego sprzyja nie tylko nowy charakter zagrożeń, ale również konsolidacja stanowiska państw Europy Środkowo-Wschodniej, postrzegających uzależnienie surowcowe od Rosji jako bezpośrednie lub pośrednie zagrożenie, oraz zmieniająca się rola Stanów Zjednoczonych na rynkach energetycznych, które stają się największym producentem węglowodorów na świecie [11]. Zakłócenia dostaw energii są elementami ataku hybrydowego, a cyberprzestrzeń jest areną wojny hybrydowej. Dlatego też, jest ona kolejnym rodzajem, po lądzie, morzu, przestrzeni powietrznej i kosmicznej, środowiskiem prowadzenia walki zbrojnej.

Co więcej, opisane możliwe działania asymetryczne w cyberprzestrzeni pozwalają na kumulowanie się i kaskadowe narastanie skutków, co przyczynia się do ich rozdzielania (dystrybuowania). Zdolność ta powoduje, że tak naprawdę żaden z wyróżnionych w jakikolwiek sposób elementów infrastruktury krytycznej atakowanego przeciwnika nie jest całkowicie odporny na oddziaływanie i każdy wygenerowany skutek emanuje na zewnątrz, wpływając na jego inne systemy lub podsystemy [23]. Niejednokrotnie w historii wojen zdarzało się, że zaplanowany skutek pierwszorzędowy generował kolejne, niezamierzone lub kompletnie nieprzewidywalne efekty pośrednie. Obecna rzeczywistość udowadnia, jak złożona jest kwestia antycypowania skutków wyższego rzędu i ich wpływu na osiąganie założonych celów.



Rys. 2. Ilustracja złożoności skutków wyższego rzędu [na podst. USAF Doctrine Center briefing, Strategic and Indirect Effects: Defining and Modeling]

Warto zwrócić uwagę, że definicje pojęcia „infrastruktura krytyczna" przyjęte przez Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych[2] i Komisję Europejską[3]

[2] Infrastruktura krytyczna to systemy ochrony fizycznej i cybernetycznej oraz kluczowe dla Stanów Zjednoczonych aktywa, których niezdolność do prawidłowego funkcjonowania lub zniszczenie wywiera wyniszczający wpływ na bezpieczeństwo kraju, w tym na bezpieczeństwo ekonomiczne lub fizyczne lub zdrowie publiczne. Krajowa infrastruktura krytyczna zapewnia niezbędne usługi, zapewniające funkcjonowanie społeczeństwa amerykańskiego (tłum. własne za: https://www.dhs.gov/what-critical-infrastructure).

[3] Infrastruktura krytyczna to zasób lub system, który jest niezbędny do utrzymania żywotnych funkcji społecznych (tłum. własne za: https://ec.europa.eu/home-affairs/what-we-do/policies /crisis -and-terrorism/critical-infrastructure_en).

są w zasadzie zbieżne i podkreślają jej szczególne znaczenie dla prawidłowego funkcjonowania gospodarki państwa i społeczeństwa. Jednocześnie, ochrona infrastruktury krytycznej w USA, a zatem posiadająca swoje kierunki i cele, wyrażone przede wszystkim w Narodowym Planie Ochrony Infrastruktury *National Infrastructure Protection Plan* [22], wprowadzonym w 2013 r. i aktualizowanym co cztery lata oraz będącym wzorcem i punktem odniesienia dla wysiłków rządu USA na rzecz ochrony infrastruktury krytycznej, nigdy nie będzie zapewniona w stu procentach. Badacze tematyki podkreślają, że pełna ochrona w tym obszarze od wszystkich potencjalnych zagrożeń i ryzyk jest niemożliwa, a cyberbezpieczeństwo wymaga dalszych badań ewaluacyjnych w kontekście oceny ryzyka i dalszej, pełnej implementacji na poziomie rządowym [6].

Mając powyższe na uwadze, warto wspomnieć kilka najważniejszych aspektów cyberataków na infrastrukturę krytyczną. Systemy sterujące są przede wszystkim podatne na hakowanie, manipulacje i wirusy, które mogą pozostać niewykryte przez miesiące, a nawet lata. W listopadzie 2011 r. Departament Bezpieczeństwa Krajowego USA i Federalne Biuro Śledcze (FBI) otrzymały informację o cyberataku na stację uzdatniania wody w Springfield w stanie Illinois. Hakerzy uzyskali dostęp do bazy danych, pobrali nazwy i hasła użytkowników systemu SCADA (Supervisory Control and Data Acquisition), co umożliwiło im zdalne sterowanie procesem technologicznym i w efekcie przegrzanie pompy wodnej [14]. Był to pierwszy, udany i potwierdzony atak tego typu na element systemu infrastruktury krytycznej w USA, a dowody w postępowaniu dochodzeniowym wskazywały, że hakerzy mogli pozostawać niewykryci w systemie już miesiąc wcześniej, zanim doszło do bezpośredniego działania. Co więcej, producenci oprogramowania sterującego często posiadają zdalny dostęp do systemów klienckich, w celu zapewnienia wysokiej jakości swoich usług, w tym np. konserwacji i aktualizacji. Jak pokazuje incydent w Springfield, może to być również „tylne wejście" dla intruzów. W przypadku Stanów Zjednoczonych częsta jest również sytuacja, w której „dobry i sprawdzony" system typu SCADA jest zapewniany przez dużego dostawcę oprogramowania nie tylko w systemach wodociągowych, ale i innych systemach infrastruktury krytycznej.

Błąd użytkownika to nadal podstawowy problem, stanowiący najczęstszą przyczynę udanych ataków na infrastrukturę sieci. W Stanach Zjednoczonych elektrownie oraz sieci energetyczne funkcjonują na poziomie regionalnym, zapewniając sobie zdecentralizowane systemy bezpieczeństwa. Jednakże, oprogramowanie podobne do wirusów komputerowych, znanych pod wspólną nazwą Stuxnet[4], może zostać wykorzystane w różnych,

[4] Stuxnet, uważany za najbardziej skomplikowany wirus komputerowy, został zaprojektowany w taki sposób, aby opanować przemysłowy system kontroli urządzeń wirowych w irańskim zakładzie wzbogacania uranu w mieście Natanz (opracowany przez firmę Siemens), celem okresowego zwiększania ich prędkości, co doprowadziło do zniszczenia. Haker, który stworzył wirusa Stuxnet dołączył go do programu użytkowego, który udostępnił na pendrive'ie kilku informatykom. Program się podobał, więc był chętnie powielany i przekazywany z rąk do rąk. W ten sposób wirus Stuxnet zakażał coraz więcej komputerów. Na każdym komputerze, do którego dotarł, Stuxnet sprawdzał, czy jest to komputer znajdujący się w irańskim zakładzie nuklearnym.

oddzielonych od siebie systemach jednocześnie. Stuxnet był pierwszym zaawansowanym narzędziem szpiegostwa przemysłowego, które wykorzystało naturalną ludzką skłonność do korzystania z darmowych programów. Wirus tego rodzaju może być dystrybuowany przez ludzi przypadkowo poprzez pamięć USB lub celowo poprzez sieć. Co więcej, do czasu kiedy władze wykryją źródło problemu, wirus może zostać zakodowany i ukryty w innych systemach w całym kraju. Nowy atak może zostać aktywowany po kilku dniach, tygodniach, a nawet miesiącach.

Z punktu widzenia bezpieczeństwa teleinformatycznego infrastruktury krytycznej, systemy sterowania przemysłowego (OT – ang. *Operational Technology*) dopiero z czasem były projektowane jako systemy oddzielne od systemów informatycznych (IT – ang. *Information Technology*). Lista różnic pomiędzy tymi dwiema grupami rozwiązań jest długa, jednak z punktu widzenia ochrony infrastruktury krytycznej kluczowe są kwestie związane z wydajnością i okresem ich działania. Z uwagi na fakt, że skutki przerwania działania systemów OT zagrażają bezpieczeństwu państwa i powodują straty finansowe nieadekwatnie wyższe od strat finansowych wynikających z braku ciągłości działania systemu IT, systemy sterowania przemysłowego stosują rozwiązania typu *real-time* w zapewnianiu dostępności procesu produkcyjnego, a średni czas ich eksploatacji to ok. 15 lat (dla systemów IT średnia to ok. 4 lat). Przy takim okresie funkcjonowania rozwiązania OT będą ograniczone przez zasoby rozumiane np. jako wydajności procesorów. Nie będą również rozwijane ich technologie i nie będzie możliwa ich rozbudowa, a w przypadku konieczności wprowadzania zmiany, będzie ona dotyczyć całego środowiska [15]. Dlatego też poziom współczesnej ochrony tych systemów zależy od szybkości wykrycia zdarzenia i szybkości (i kompletności) odpowiedzi na nie przy zachowaniu ciągłości działania istotnych procesów. To z kolei zapewniają wyłącznie nowoczesne rozwiązania teleinformatyczne. Według raportu Instytutu Kościuszki z 2014 r., poświęconego w całości kwestiom bezpieczeństwa infrastruktury krytycznej, trudno sobie dziś wyobrazić, w jaki inny sposób można realizować działania ochronne bez wdrażania rozwiązań ICT równolegle do istniejących w przemyśle systemów ICS (ICS – ang. *Industrial Control Systems*, np. SCADA). Wymiana danych pomiędzy tymi systemami pozostaje wciąż otwarta, jednak głównym powodem wprowadzania zmiany technologicznej w zakresie zabezpieczeń cybernetycznych OT jest ekonomika ich użyteczności. Środowisko automatyki przemysłowej coraz bardziej otwiera się na systemy cybernetyczne i zbliżenie do świata IT głównie poprzez konwergencje na poziomie infrastruktury (np. serwery i stacje dyspozytorskie), komunikacji (protokoły przemysłowe zastępowane przez standard TCP/IP) czy systemów operacyjnych [10, 25, 26].

Jeśli był to dowolny inny komputer, Stuxnet nie wyrządzał żadnych szkód, przez co pozostawał niezauważony, jedynie produkował oraz rozsyłał swoje kopie. Szacuje się, że w sumie zakażonych zostało kilkaset tysięcy komputerów [20, 24].

Niezbędne jest ramowe podejście do ochrony infrastruktury krytycznej oraz wprowadzanie nowych standardów dotyczących kwestii bezpieczeństwa wobec asymetrycznych zagrożeń możliwych hybrydowych wojen przyszłości. W anglojęzycznej literaturze badawczej problematyki cyberbezpieczeństa w obszarze ochrony infrastruktury krytycznej stosuje się termin *resilience* (odporność). Powoli termin *resilience* znajduje swoje miejsce w podstawowych założeniach narodowych programów, polityki i strategii, jednakże narodowe podmioty operujące zasobami infrastruktury krytycznej nie mogą ograniczać się do rozumienia *resilience* jako działań ad hoc. To nie jest już tylko kwestia technologii, ale także zarządzania organizacją i wiedzą[5] w szczególnie zhierarchizowanych i skomplikowanych strukturach oraz środowisku wysoce ze sobą rywalizującym. Celem *resilience* jest bowiem identyfikowanie zagrożeń, na długo zanim staną się one negatywnymi zdarzeniami, a sytuacją idealną jest osiągnięcie efektywnego poziomu zarządzania i dzielenie się wiedzą pomiędzy hierarchicznymi strukturami państwowymi i konkurującymi ze sobą podmiotami prywatnymi.

Estonia od wielu lat służy jako przykład pierwszej ofiary cybernetycznej wojny, w której hakerom zależało na uzyskaniu efektów psychologicznych, np. poprzez zawieszenie usług bankowych i odizolowanie państwa od reszty świata. By wyobrazić sobie skalę ataku z 2007 r., wystarczy przytoczyć słowa ówczesnego prezydenta Estonii Toomasa Hendrika Ilvesa, który stwierdził: „W obecnych czasach nie potrzeba pocisków, żeby zniszczyć infrastrukturę. Można to zrobić online" [18]. Wówczas rozpoczęto dyskusję, czy artykuł piąty Karty NATO dotyczy także cyberterroryzmu [7]. Na przykładzie haktywistów, ich niewykrywalności i skutków, jakie mogą spowodować ich działania, atak z 2007 r. pokazuje, że parasol ochronny w postaci NATO czy Stanów Zjednoczonych nie gwarantuje suwerenności państwowej w cyberprzestrzeni. Jeśli zaś ataki na serwery rządowe wywołują panikę na tak wielką skalę, cyberataki na infrastrukturę krytyczną stanowią nieporównywalnie większe zagrożenie dla bezpieczeństwa całego państwa oraz zdrowia i życia jego obywateli.

Cyberbezpieczeństwo musi być zarządzane w taki sam sposób, jak realizowana jest formuła *lessons learned,* a nowe sposoby myślenia i adaptowania rozwiązań mogą być naśladowane. Stany Zjednoczone, uważane za światowego lidera cyberbezpieczeństwa, wciąż samokrytycznie podchodzą do problemu przygotowania państwa na poważne cyberataki. Po części wynika on z potężnego obszaru instytucjonalnego i systemowego podatnego na ewentualne incydenty (Departament Obrony, potężny sektor finansowy, szczególnie podatne i przestarzałe systemy ochrony infrastruktury krytycznej,

[5]Ponad 70% cyberataków kończy się sukcesem z powodu niestosowania przez użytkowników systemów podstawowych zasad tzw. cyber-higieny: zmiany haseł, unikania używania pamięci USB z nieznanych źródeł, umiejętności rozpoznania elementarnych fragmentów ataku phisingowego itp. Edukacja opinii publicznej na wszystkich poziomach, począwszy od szkoły podstawowej będzie mieć znaczący wpływ na zredukowanie podatności i słabości czynnika ludzkiego w cyberprzestrzeni [17].

tj. elektrownie, tamy, mosty, gazociągi itp., a także szpitale i obiekty przechowujące dane osobowe), a po części z rozproszenia podmiotów odpowiedzialnych za realizację rządowych strategii cyberbezpieczeństwa. Istnieje bowiem sześć oddzielnych centrów cyberbezpieczeństwa w rządzie i żaden nie odgrywa roli wiodącej [17].

Od wielu lat rządy wprowadzają własne strategie reagowania na incydenty bezpieczeństwa infrastruktury krytycznej w celu znalezienia najlepszych, systemowych rozwiązań przeciwdziałania zagrożeniom asymetrycznym. Choć nie każda doktryna, polityka czy strategia jest taka sama, to jednak założenia są najczęściej tożsame – włączenie teorii militarnego odstraszania w kontekst ofensywnych cyberoperacji we wszystkich obszarach bezpieczeństwa państwa, w tym ochrony infrastruktury krytycznej. Więcej, cyberprzestępczość musi zostać uwzględniona w systemie prawnych sankcji państwa, a pojęcie „cyberatak" musi zostać zdefiniowane w doktrynie międzynarodowych stosunków politycznych, gospodarczych i społecznych. Już w 2010 r. rząd Australii wprowadził interesującą instrukcję wskazującą sposoby zarządzania wobec wyzwań cybernetycznych dla infrastruktury krytycznej. Australijska „Strategia Odporności Infrastruktury Krytycznej" (ang. Critical Infrastucture Resilience Strategy) zachęca wszystkie organizacje (państwowe i prywatne) do rozwijania organicznej zdolności radzenia sobie z nagłym atakiem, zamiast stosowania tradycyjnego podejścia rozwijania planów radzenia sobie z atakiem, w ramach policzalnych scenariuszy, szczególnie w kontekście rosnącej złożoności środowiska [2]. Celem rządu jest zatem nakazanie podmiotom rozwijania metod i ćwiczeń do poprawienia zdolności reagowania na incydenty, których po prostu nie spodziewamy się. Opracowywanie planów kryzysowych jest działaniem elementarnym, szczególnie na rzecz zdarzeń, które mogą występować. W szerszym kontekście, należy rozpocząć dyskusję o rozwijaniu zdolności na przeciwdziałanie katastroficznym „niespodziankom", które mogą przesłonić konwencjonalne możliwości instytucjonalne. Jak zatem przygotować się do czegoś, czego przewidzieć się nie da?

3. Wnioski

Zarządzanie wiedzą, lepsza organizacja instytucji zajmującej się kwestiami cybersecurity (lub wyłonienie jednej wiodącej instytucji) oraz ciągłe nabywanie wiedzy to niezbędny warunek skutecznego wdrażania rozwiązań z obszaru cyber w sektorze prywatnym i państwowym, w tym państw NATO. Stany Zjednoczone wiedzą, że miliardy inwestowane przez rząd oraz sektor prywatny w rozwiązania technologicznie nie mają znaczenia, o ile obydwa sektory nie będą działać wspólnie w silnej współpracy publiczno-prywatnej. Zagrożenia będą bowiem ewoluować i zmieniać się z biegiem czasu. Tak jak „skaczące bomby" były innowacyjnym rozwiązaniem, tak kolejne sposoby ataków będą innowacyjnym wyzwaniem dla cyberbezpieczeństwa. Nowe rozwiązania będą przygotowywać narodowych operatorów do nietypowych sytuacji, których nie można przewidzieć. Wspomniana *resilience* wymaga nowych metod unikania takich sytuacji

w pierwszej kolejności. Należy pamiętać, że cyberatak na obiekty infrastruktury krytycznej jest rzeczą niezwykle groźną dla wysokorozwiniętych państw, uzależnionych od sprawnego funkcjonowania systemów informacyjnych. Może on doprowadzić nie tylko do olbrzymich strat gospodarczych czy niepokojów społecznych (a w efekcie do kryzysu rządowego), ale także mogą osłabić armię przeciwnika w przypadku konieczności podjęcia realnej walki zbrojnej. Oznacza to, iż znacznie zostaje obniżona niezawodność funkcjonowania organizmu państwowego jako sprawnego systemu.

4. Literatura

1. Biedrzycki J., Wiśniewski K.: Awaria we Włoszech z 28.09.2003 r. – raport, Biuletyn Urzędu Regulacji Energetyki, nr 4/2004, www.cire.pl/pliki/2/wawaria.pdf.
2. Critical Infrastructure Resilience Strategy, www.tisn.gov.au/documents/Australian+government+s+critical+infrastructure+resilience+strategy.pdf, (dostęp: 27.01.2019 r.).
3. Dżihadyści zaatakowali największą rafinerię w Iraku, www.energetyka24.com/dzihadysci-zaatakowali-najwieksza-rafinerie-w-iraku (dostęp: 17.12.2018 r.).
4. Gołota M.: Wybuchowe beczki i potop w Zagłębiu Ruhry. Tajemnica sukcesu operacji „Chastise", Polska the Times, 21 maja 2013 r., https://polskatimes.pl/wybuchowe-beczki-i-potop-w-zaglebiu-ruhry-tajemnica-sukcesu-operacji-chastise-zdjecia/ar/900228 (dostęp: 6.12.2018 r.).
5. Greenpeace protest over Greenland oil drilling ended, BBC News, 7.07.2011 r., https://www.bbc.com/news/uk-scotland-13653370 (dostęp: 6.12.2018 r.).
6. Hemme K.: Critical Infrastructre Protection Maintenance is National Security. Journal of Strategic Security 2015, Vol. 8, No. 3, Supplement: Eleventh Annual IAFIE Conference, University of South Florida Board of Trustees.
7. Herzog S.: Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, Vol 4, No. 2, 2011.
8. Milewski J.: Identyfikacja infrastruktury krytycznej i jej zagrożeń. Zeszyty Naukowe AON nr 4(105) 2016.
9. Kerigan-Kyrou D.: Critical Energy Infrastructure Operators, NATO and Facing Future Challenges, Partnership for Peace Consortium of Defense Academies and Security Studies Institutes. Connections, Vol. 12, No. 3, 2013.
10. Kotłowski W.: Teleinformatyczne elementy ochrony infrastruktury krytycznej. W: J. Świątkowska (red.), Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny, Instytut Kościuszki, Kraków 2014.
11. Kozłowski G., Wieczorkiewicz J.: Bezpieczeństwo energetyczne NATO: historia, doktryny i perspektywy rozwoju. Bezpieczeństwo Narodowe, nr 37-40, I-IV, Wyd. Biuro Bezpieczeństwa Narodowego, Warszawa 2016.
12. Marud W.: Targeting w teorii Sił Powietrznych. Akademia Obrony Narodowej, Wydział Zarządzania i Dowodzenia, 2008.

13. Milewski J.: Identyfikacja infrastruktury krytycznej i jej zagrożeń. Zeszyty Naukowe AON nr 4(105) 2016.
14. Nakashima E.: Foreign hackers targeted U.S. water plant in apparent malicious cyber attack, expert says. Washington Post, 18.11.2011 r. www.washingtonpost.com/blogs/checkpoint-washington/post/foreign-hackers-broke-into-illinois-water-plant-control-system-industry-expert-says/2011/11/18/gIQAgmTZYN_blog.html?noredirect=on&utm_term=.d20001793ce4 (dostęp: 14.04.2019 r.).
15. Ryba M.: Rola elementów teleinformatycznych w funkcjonowaniu infrastruktury krytycznej. W: J. Świątkowska (red.), Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny, Instytut Kościuszki, Kraków 2014.
16. Strategic and Indirect Effects: Defining and Modeling. USAF Doctrine Centre, www.doctrine.af.mil/application/issues/strateffects.pdf (dostęp 10.05.2006 r.).
17. Stavridis J.: The United States is not ready for a Cyber-Pearl Harbor. 15 maja 2017, Foreign Policy https://foreignpolicy.com/2017/05/15/the-united-states-is-not-ready-for-cyber-pearl-harbor-ransomware-hackers-wannacry/ (dostęp: 1.02.2019 r.).
18. Stolarczyk J.: Estonia – pierwsza ofiara cybernetycznej wojny, 17.02.2017 r., https://wiadomosci.onet.pl/tylko-w-onecie/estonia-pierwsza-ofiara-cybernetycznej-wojny/t3czdg5 (dostęp: 18.03.2019 r.).
19. Streeter M.: IRA team who planned terror blitz on capital given 35 years. The Independent, 3.07.1997 r., www.independent.co.uk/news/ira-team-who-planned-terror-blitz-on-capital-given-35-years-1248661.html (dostęp: 18.12.2018 r.).
20. Stuxnet, najgroźniejszy wirus świata. Czy to dzieło izraelskiego wywiadu?, 3.10.2010 r., www.newsweek.pl/swiat/stuxnet-wirus-robak-stuxnet/z4zeec3, (dostęp: 13.03.2019 r.).
21. Świerczyńska K.: Terror na morzu, www.focus.pl/artykul/terror-na-morzu (dostęp: 11.12.2018 r.).
22. The National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience, www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.
23. Rinaldi S.M.: Beyond the Industrial Web: Economic Synergies and Targeting Methodologies. School of Advanced Airpower Studies, Maxwell 1995.
24. Zieja M., Smoliński H., Gołda P.: Information systems as a tool for supporting the management of aircraft flight safety, Archives of TransportVolume 36, Issue 4, 2015, Pages 67-76.
25. Zieja M., Ważny M., Stępień S.: Outline of a method for estimating the durability of components or device assemb.lies while maintaining the required reliability level. Eksploatacja i Niezawodnosc – Maintenance and Reliability, Volume 20, Issue 2, 2018, Pages 260-266.
26. Zieja M., Woch., Tomaszewska J.: Analysis of the time between failures of aircrafts, 2nd International Conference on System Reliability and Safety, ICSRS 2017, Volume 2018-January, 29 January 2018, Pages 112-118.