AKADEMIA
OBRONY
NARODOWEJ

Projekt badawczy 0500A 01923:
MODELOWANIE ZAGROŻEŃ DLA BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA. TEORIA WALKI INFORMACYJNEJ

MODELOWANIE WALKI INFORMACYJNEJ

(Podstawy, scenariusze, modele)

Tom II

Raport z badań

WARSZAWA

AKADEMIA OBRONY NARODOWEJ

Projekt badawczy 0500A 01923:
MODELOWANIE ZAGROŻEŃ DLA BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA. TEORIA WALKI INFORMACYJNEJ

MODELOWANIE WALKI INFORMACYJNEJ

(Podstawy, scenariusze, modele)

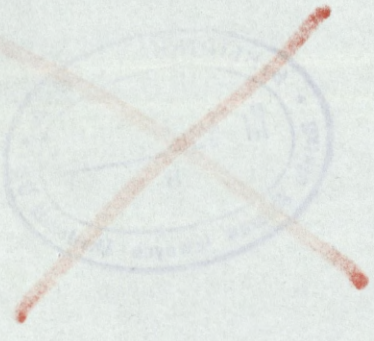
Tom II

Raport z badań

Warszawa **2004**

Opracował zespół autorski:

Gen. broni prof. dr inż. Tadeusz **JEMIOŁO**	**T.I. roz. 1.2.**
Płk prof. dr hab. inż. Piotr **SIENKIEWICZ**	**T.I. roz. 1.1., 1.9.,1.10., T.II.roz.1.1.**
Płk dr hab. Ryszard **SZPYRA**	**T.I roz.1.3. T.II.roz.2.2., 2.3.**
Mjr dr hab. Henryk **SPUSTEK**	**T.I. roz. 1.8.**
Płk dr inż. Marek **KINASIEWICZ**	**T.I. roz. 1.6. T.II. roz.2.4.**
Płk dr inż. Marian **URBANEK**	**T.I. roz. 1.7.**
Ppłk dr inż. Janusz **WOCIAL**	**T.I. roz. 1.7.**
Ppłk dr inż. Piotr **GÓRNY**	**T.I. roz. 1.4.**
Ppłk dr inż. Wiesław **BŁAŻEJCZYK**	**T.III roz.1.,3.,4.**
Mjr mgr inż. Jan **KUCHARSKI**	**T.I. roz. 1.5. T.III.roz.4.,5.**
Kpt. mgr inż. Jerzy **GRZYB**	**T.III. roz.2.,4.**
Mgr Halina **ŚWIEBODA**	**T.I. roz.1.9. redakcja całości**



Spis treści

2.1. TEORETYCZNE PODSTAWY WALKI INFORMACYJNEJ

2.1.1. Cybernetyka walki – wprowadzenie

Wszelkie zorganizowane działania, rozpatrywane zarówno w kategoriach kooperacji pozytywnej, jak i kooperacji negatywnej (T. Kotarbiński) wymagają celowego użycia potencjału ludzkiego i materialno-energetycznego oraz potencjału informacyjnego. Sterowanie działaniami jest z natury procesem informacyjno-decyzyjnym, polegającym na oddziaływaniu obiektu sterującego na obiekt sterowany w celu wywołania w nim zmian pożądanych i przeciwdziałania zmianom niepożądanym. Sterowanie wymaga odpowiednich zasobów informacyjnych, dysponowanie którymi wiąże się z realizacją procesów:

- pozyskiwania (zdobywania) informacji,
- przesyłania informacji,
- przechowywania informacji,
- przetwarzania informacji,
- udostępniania informacji,

zgodnie z potrzebami i wymaganiami określonych użytkowników (ośrodków decyzyjnych).

Procesy informacyjne są (mogą być) obiektem zewnętrznych oddziaływań destrukcyjnych (zagrożeń) takich jak:

- losowe: przewidywalne i trudno przewidywalne,
- deterministyczne: kumulacyjne i **świadome**.

Zagrożenia losowe, będące rezultatem np. zmian środowiskowych (np. zmiana warunków propagacji fal radiowych), mogą wpływać np. na obniżenie jakości przesyłania informacji. Współczesna telekomunikacja stworzyła jednak efektywne systemy zabezpieczenia zapewniające wysoką jakość transakcji.

Zagrożenia deterministyczne mogą być rezultatem kumulacji wielu procesów, z których każdy z osobna nie stanowi istotnego zagrożenia, lecz ich kumulacja w określonym miejscu i czasie takim zagrożeniem (np. dla bezpieczeństwa systemów informacyjnych) się staje.

Natomiast zagrożenia świadome są efektem zorganizowanego działania, którego celem jest destrukcja, tzn. zniszczenie lub zmniejszenie efektywności

systemów informacyjnych (lub ich elementów), albo określonych obiektów tworzących tzw. infrastrukturę krytyczną. Stanowią one nowe wyzwanie dla odpowiedzialnych za bezpieczeństwo państwa, gotowość systemów informacyjnych, zarządzanie zasobami informacyjnymi itp.

Ostatni z wymienionych typów zagrożeń dla bezpieczeństwa informacyjnego stanowi istotę **walki informacyjnej**. Walka informacyjna **zawsze** była istotnym elementem **walki zbrojnej**. Postęp w dziedzinie **technologii informacyjnych** przyniósł takie **jakościowe zmiany,** jak:

- wzrost różnorodności rodzajów i typów zagrożeń informacyjnych;
- wzrost „kompleksowości" zagrożeń, tj. wzrost liczby typów i rodzajów obiektów zagrożeń informacyjnych;
- wzrost intensywności informacyjnych oddziaływań destrukcyjnych;
- wzrost autonomiczności niektórych form walki informacyjnej, tj. uzyskanie „statusu samodzielnego" środka osiągania celów militarnych;
- globalizacja systemów informacyjnych;
- powstanie „przestrzeni cybernetycznej" i nadanie jej rangi jednego z wymiarów walki (model Wardena).

Konceptualizacja

Przyjęte ogólne założenia nawiązują do dawnej propozycji J. Koniecznego *„Cybernetyki walki"* (1970). Należy zwrócić uwagę na zawartą tam jakże trafną antycypację współczesnych koncepcji *„Cyberwar"*.

Cybernetyczne ujęcie zjawiska walki informacyjnej wynika z następujących przesłanek:

- **sterowanie** i **informowanie** na potencjalnym polu walki znajduje się w centrum uwagi;
- **obiekty** zaangażowane w procesy walki informacyjnej charakteryzowane są za pomocą określonych wejść i wyjść informacyjnych, zarówno pozytywnych, jak i negatywnych (destrukcyjnych);
- każdy rozpatrywany obiekt cechuje określony **potencjał** i potencjalna **efektywność** (skuteczność, żywotność, gotowość, ekonomiczność), zaś zasoby posiadają **wartość** – ocenianą z różnych punktów widzenia (np. ich dysponenta i przeciwnika);

- każdy obiekt (proces, system) rozpatrywany jest w określonym **kontekście** – relacjach z otoczeniem (zarówno w sensie kooperacji pozytywnej, jak i kooperacji negatywnej);
- **informowanie** (proces informacyjny) może posiadać charakter:
  - **transinformowania** (informowania wiernego),
  - **pseudoinformowania** (np. informowania pozornego, rozwlekłego itp.),
  - **dezinformowania** (informowania fałszywego zmierzającego do wprowadzenia w błąd przeciwnika),
  - **metainformowania** (informowania i informowaniu).
- ze względu na bezpieczeństwo informacyjne informacja posiada **atrybuty** takie, jak:
  - **tajność** *(confidentiality),*
  - **integralność** *(integrity),*
  - **dostępność** *(availability).*

Przyjęto następujące ogólne **założenia:**

(1) „sytuacja → sytuacja konfliktowa → konflikt → walka → walka informacyjna", co oznacza, że pojęcia *„sytuacji"* i *„konfliktu"* przyjęto za punkt wyjścia do operacjonalizacji pojęcia *„walki informacyjnej".*

(2) „ walka informacyjna → równowaga informacyjna → przewaga informacyjna → asymetria informacyjna".

(3) „ bezpieczeństwo informacyjne → niebezpieczeństwo informacyjne → ryzyko informacyjne → zagrożenia informacyjne".

(4) „ilość informacji → jakość informacji → użyteczność informacji →koszt informacji → wartość informacji".

(5) „polityka bezpieczeństwa → strategia bezpieczeństwa informacyjnego → środki zabezpieczenia".

Definicje:

D1. Sytuacją nazywamy ciąg relacji pomiędzy obiektem (systemem) a jego otoczeniem określonych w danej chwili (okresie) czasu.

D2. Sytuacją konfliktową nazywamy sytuacje taką, że wśród relacji między obiektem a jego otoczeniem istnieją relacje o charakterze kooperacji negatywnej (sprzężeń destrukcyjnych).

D3. Konfliktem nazywać będziemy przeciwstawne działania dwóch lub więcej obiektów, wynikające z ich wzajemnie sprzecznych celów (interesów).

D4. Walką jest każda sytuacja konfliktowa, której uczestnicy (obiekty) dążą do osiągnięcia swoich celów stosując dowolne, dopuszczalne strategie i wynikające z nich środki.

D5a. Walką informacyjną nazywać będziemy taka formę walki, której uczestnicy bądź stosują środki oddziaływania informacyjnego, bądź obiektem ich działania nieinformacyjnego (energomaterialnego) są obiekty (systemy) informacyjne strony przeciwnej.

D5b. Walką informacyjną nazywać będziemy całokształt działań ofensywnych i defensywnych, prowadzących do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych).

D5c. Walką informacyjną są działania konieczne do:

- zniszczenia (lub degradacji wartości)zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych,
- zapewnienia bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych.

D6a. Równowagą informacyjną nazywamy nazywać będziemy taki stan sytuacji konfliktowej, który charakteryzuje brak przewagi informacyjnej którejkolwiek ze stron uczestniczących w tej sytuacji.

D6b. Równowagą informacyjną nazywać będziemy stan sytuacji polegający na istnieniu pełnej symetrii informacji, czyli pełnej wzajemnej kontroli działań (wzajemnej znajomości wartości potencjałów, ich przestrzegania i czasowego rozkładu, celów działania itp.).

D7a. Przewagą informacyjną nazywamy taki stan sytuacji konfliktowej, w której jedna ze stron posiada większą efektywność systemów informacyjnych i wynikającą stąd zdolność do tworzenia lepszych, niż strona przeciwna, warunków do osiągnięcia swoich celów (różnica w efektywności systemów dowodzenia, łączności, rozpoznania, walki elektronicznej itp.).

D7b. Przewaga informacyjną nazywać będziemy stan sytuacji charakteryzujący się asymetrią informacji, tj. jedna ze stron dysponuje większą wiedzą („lepszymi" informacjami sytuacyjnymi) niż strona przeciwna.

D8. Asymetria informacji charakteryzuje taki stan sytuacji, w którym istnieje nierównomierny podział (dostęp) informacji, zaś strona „poinformowana" dąży

do strategicznego wykorzystania swojej przewagi informacyjnej nad strona „niedoinformowaną".

D9. Bezpieczeństwem informacyjnym nazywać będziemy taki stan systemu, który charakteryzuje się pożądanym poziomem zabezpieczenia przed zagrożeniami informacyjnymi.

D10. Niebezpieczeństwem informacyjnym nazywać będziemy taki stan systemu, który charakteryzuje niespełnienie wymaganego poziomu bezpieczeństwa informacyjnego (system charakteryzuje podatność na zagrożenia, wysoki stopień ryzyka).

D11. Ryzyko informacyjne jest charakterystyką systemu wyrażającą zwiększone prawdopodobieństwa wystąpienia strat wartości obiektów spowodowanych zagrożeniami informacyjnymi (wysoki poziom podatności na zagrożenia dla bezpieczeństwa).

D12. Zagrożeniem informacyjnym nazywać będziemy każde możliwe i prawdopodobne oddziaływania strony przeciwnej, której celem jest: utrata atrybutów informacji istotnych dla systemu, spowodowanie degradacji wartości jego zasobów informacyjnych i spadek efektywności jego systemów informacyjnych lub zniszczenie informacyjnej infrastruktury systemu.

D13. Ilość informacji jest charakterystyką informacji wyrażającą zdolność zmniejszenia niepewności sytuacji określonego użytkownika, pozwalającą na podjęcie przez niego celowego działania.

D14. Jakość informacji jest kompleksową charakterystyką wyrażającą aktualność informacji, jej pełność (kompletność), wiarygodność i przyswajalność, rozpatrywaną w kontekście wymagań konkretnego użytkownika.

D15. Użyteczność informacji jest cechą wyrażająca jej wpływ na wzrost efektywności (skuteczności) działania konkretnego użytkownika.

D16. Koszt informacji jest cechą wyrażającą łączne koszty pozyskania informacji, jej przesłania, przechowywania, przetwarzania i udostępniania.

D17. Wartość informacji jest kompleksową charakterystyką – określoną relacją (funkcją) między użytecznością informacji a jej kosztem.

D18. Polityką bezpieczeństwa informacyjnego nazywać będziemy całokształt przedsięwzięć związanych z zarządzaniem i ochroną informacji oraz systemów informacyjnych, a także metodami (procedurami) przeciwdziałania zagrożeniom informacyjnym.

D19. Strategią bezpieczeństwa informacyjnego nazywać będziemy wybór metod i środków zabezpieczenia (ochrony i obrony) – przeciwdziałania zagrożeniom informacyjnym.

D20. Środkami zabezpieczenia (bezpieczeństwa) określać będziemy takie środki (zasoby, metody) organizacyjne, techniczne i programowe, których zastosowanie zwiększa poziom bezpieczeństwa informacyjnego (lub zmniejsza podatność na zagrożenia informacyjne).

D21. Zarządzanie bezpieczeństwem informacyjnym obejmuje całokształt przedsięwzięć pozwalających na wybór takiej strategii bezpieczeństwa informacyjnego, która gwarantuje osiągnięcie pożądanego poziomu bezpieczeństwa informacyjnego obiektu (systemu).

D22. Optymalizacja bezpieczeństwa informacyjnego polega na poszukiwaniu takiej strategii bezpieczeństwa informacyjnego, która zapewni:

- minimalny stopień ryzyka przy kosztach zabezpieczeń nie większych od wartości kosztów granicznych (dopuszczalnych) lub
- maksymalny poziom bezpieczeństwa (minimalny poziom ryzyka) przy założeniu najmniej korzystnych warunków działania.

2.1.2. Modelowanie walki informacyjnej

Model zagrożenia

Rozpatruje się **sytuację** systemową

$$\Sigma = \langle S,O,R \rangle$$

gdzie: S – system będący **obiektem** zagrożeń;

O – otoczenie, które tworzą obiekty będące **źródłem** zagrożeń;

$R \subset S \times O$ – zbiór relacji.

Obiekt zagrożeń charakteryzuje jego potencjał obronny (zabezpieczający): $P(s) \geq 0$, $s \in S$.

Źródło zagrożeń charakteryzuje jego potencjał destruktywny: $P(o) \geq 0$, $o \in O$.

Na zbiorze R określono **relację zagrożenia** Rz = Rz (o,s), taką że:

$$\bigwedge_{o,s} o \, Rz \, s \Leftrightarrow P(o) \geq P(s)$$

czyli obiekt $s \in S$ jest zagrożony przez $o \in O$.

Relacją zagrożenia może być funkcja Rz(t) czasu rzeczywistego $t \in T$.

Stan zagrożenia można interpretować jako punkt na płaszczyźnie zespolonej Gaussa opisanej współrzędnymi P(o), P(s), czyli $z = z(o,s) \overset{df}{=} \langle P(o), P(s) \rangle$, załóżmy, że każdemu $t \in T$ można przypisać liczbę zespoloną

$$Z(t) = P(o,t) + i\,P(s,t)$$

a wtedy zbiór punktów opisanych równaniem $z = z(t)$ można interpretować jako trajektorię stanów pewnej **sytuacji zagrożenia.**

Trajektoria może mieć następujące charakterystyczne przebiegi:

a) Jeżeli relacja Rz(t) zachodzi dla każdego $t \in T$, czyli $\text{Im } z(t) \leq \text{Re } z(t)$, to wówczas trajektoria z =(t) jest **trajektorią zagrożenia.**

b) Jeżeli relacja Rz(t) nie zachodzi dla żadnego $t \in T$, to wówczas trajektoria $z = z(t) = b(t)$ jest **trajektorią bezpieczeństwa.**

Pomiędzy trajektorią z(t) a osią t można rozpiąć powierzchnię zagrożenia $\Pi(z(t))$, natomiast pomiędzy trajektorią b(t) a osią t można rozpiąć powierzchnię bezpieczeństwa $\Pi(b(t))$. Obie te powierzchnie tworzą całość. Analiza tego modelu pozwala na rozpatrywanie sytuacji zagrożenia w kategoriach teorii katastrof.

Analiza systemowa sytuacji zagrożenia może być „skalowana" według dwóch **kryteriów oceny:**

a) kryterium prawdopodobieństwa zaistnienia stanu zagrożenia (lub innej miary charakteryzującej możliwość wystąpienia zagrożenia, np. miary rozmytej),

b) kryterium powagi (*severity*) stanu zagrożenia (np. **ryzyko** oraz **wartość** zabezpieczanego systemu lub wartość dysponowanych przez niego zasobów).

Model bezpieczeństwa

Rozpatrzmy, jak poprzednio, pewną sytuację systemową Σ oraz załóżmy, że dane są wielkości:

- zagrożenia zewnętrzne A(t) pochodzące z otoczenia (O) systemu (S),
- odporność systemu (S) na zagrożenia zewnętrzne B(t), która odpowiada funkcji potencjału obronnego (zabezpieczającego).

Powyższe charakterystyki sytuacji są funkcjami losowymi o znanych rozkładach prawdopodobieństwa:

$$F(a,t) = \Pr\{ A(t) < a \},\ a \geq 0,$$

$$G(b,t) = \Pr\{ B(t) < b \}\ b \geq 0,$$

$$t \in T.$$

Uogólnionym wskaźnikiem bezpieczeństwa systemu może być prawdopodobieństwo, że zagrożenia nie przekroczą pewnego krytycznego (dopuszczalnego) poziomu $a_o \geq 0$, zaś odporność systemu będzie większa od pewnej wartości granicznej b_o, czyli

$$\beta(t) \equiv \beta(a_o, b_o) = Pr\{A(t) \leq a_o, B(t) > b_o\}$$

co przy założeniu statystycznej niezależności rozpatrywanych wielkości prowadzi do wskaźnika oceny bezpieczeństwa systemu:

$$\beta(t) = F(a_o, t)\,[1 - G(b_o, t)]$$

Przyjmując pożądany poziom bezpieczeństwa systemu jako $\beta_o > 0$ powiemy, że w czasie T system jest bezpieczny, jeżeli w każdej chwili $t \in T$ spełniony jest warunek:

$$\beta(t) \geq \beta_o.$$

Jeżeli przyjmiemy, że niebezpieczną (kryzysową) sytuacją systemową jest sytuacja określona następująco:

$$(A(t) > a_o, B(t) \leq b_o),$$

to możemy przyjąć, że wskaźnikiem bezpieczeństwa systemu jest prawdopodobieństwo tego, że w określonym czasie nie powstaną sytuacje niebezpieczne dla systemu.

Model ryzyka

Załóżmy, że możliwe i prawdopodobne zagrożenia zewnętrzne dla systemu $Z = \{ z_i : i = 1,2,...,N\}$ mogą przynosić w czasie T straty wartości systemu (lub jego zasobów) odpowiednio: $W_i = w(Z_i)$, $i = 1,2,..., N$, przy czym dane są prawdopodobieństwa ich wystąpienia w czasie T:

$$p_i \equiv Pr\{z_i\},\ p_i \geq 0,\ \sum_{i=1}^{N} p_i = 1.$$

Na podstawie powyższych danych określa się następujące charakterystyki skutków zagrożeń zakładając niezależność skutków wystąpienia zagrożeń oraz, że i – te zagrożenie dotyczy obiektu i-tego o wartości V_i, przy czym $V_i - W_i \geq 0$:

- wartość oczekiwana:

$$\bar{W} = \sum_{i=1}^{N} p_i W_i$$

- wariancja:

$$\mathrm{var}(w) = \sum_{i=1}^{N} p_i (W_i - \bar{W})^2$$

- odchylenie standardowe:

$$\Delta(w) = \sqrt{\mathrm{var}(w)}$$

- współczynnik zmienności:

$$r = \frac{\Delta(w)}{\bar{w}}$$

wtedy, jako wskaźnik (miarę) ryzyka związanego z zagrożeniami (destrukcyjnym oddziaływaniem otoczenia systemu) przyjmuje się wartość współczynnika zmienności r. Model ten dotyczy przypadku rozpatrywania systemu jako pasywnego obiektu zagrożeń.

Model zabezpieczenia

Załóżmy, że w chwili t = 0 wartość systemu wynosi $v_o > 0$ i równa się sumie wartości poszczególnych elementów (podsystemów), czyli:

$$v_o = \sum_{j=1}^{M} v_{jo}$$

Znany jest zatem rozkład wartości w strukturze systemu S:

$$\langle \upsilon_{10}, \upsilon_{20}, \ldots, \upsilon_{jo}, \ldots, \upsilon_{jm} \rangle$$

gdzie $\upsilon_{jo} = \frac{v_{jo}}{v_o}$.

Otoczenie generuje zagrożenia skierowane na system $Z \to S$, przy czym wartość oczekiwana strat w obiekcie $S_j \in S$ w wyniku wystąpienia zagrożenia $Z_i \in Z$ wynosi W_{ij}, $0 \le W_{ij} \le v_{ij}$. Jeżeli założymy, że do chwili t wystąpiło N zagrożeń oraz, że teoretycznie na każdy obiekt mogą być skierowane wszystkie możliwe i prawdopodobne zagrożenia, to w chwili t wartość obiektu S_j wyniesie

$$v_{jt} = v_{jo} - \sum_{i=1}^{N} W_{ij} \ge 0$$

wartość systemu po „zmasowanym" zagrożeniu wyniesie

$$v_t = \sum_{j=1}^{M} v_{jt} = \sum_{j=1}^{M} \left(v_{jo} - \sum_{i=1}^{N} W_{ij} \right)$$

przy czym straty systemu wyniosą: $v_o - v_t \ge 0$.

Niech decyzję otoczenia – określa zmienna:

$$x_{ij} = \begin{cases} 1, \text{ jeśli zagrożenie } Z_i \text{ skierowane zostało na obiekt } S_j, \\ 0, \text{ w przeciwnym wypadku} \end{cases}$$

czyli określa się „przydział" poszczególnych zagrożeń do poszczególnych obiektów, przy czym spełnione muszą być warunki:

$$\sum_{j=1}^{M} x_{ij} = 1, i = 1,...,N$$

$$\sum_{i=1}^{N} x_{ij} = 1, j = 1,...,M$$

$$\sum_{i=1}^{N}\sum_{j=1}^{M} x_{ij} \le M \le N$$

Wtedy funkcja wartości systemu w chwili t ma postać

$$v_t(x) = \sum_{j=1}^{M}\left(v_{jo} - \sum_{i=1}^{N} W_{ij} X_{ij} \right)$$

Strategia ataku na system:

Otoczenie dokonuje wyboru takiego „przydział" zagrożeń na elementy systemu, który minimalizuje wartość systemu w chwili t, czyli:

$$\min v_t(x) = v_t(x^*)$$
$$x \in X$$

gdzie X – zbiór dopuszczalnych decyzji otoczenia x^* - optymalna strategia ataku na pasywny system, tj. nie dysponujący środkami obrony (ochrony).

Załóżmy obecnie, że system dysponuje środkami przeciwdziałania zagrożeniom (środkami obrony i ochrony) określonymi zbiorem B = {B_k: k=1,2,...,K}.

Użycie środka B_k przeciw zagrożeniu powoduje zmniejszenie jego skutków (start obiektu) o wartość określoną pewna funkcją.

$f_{ijk} = f(W_{ij}, b_{ijk}) \ge 0$, gdzie b_{ijk} - wielkość „osłabienia" oddziaływania zagrożenia Z_i na obiekt S_j zabezpieczony przez B_k. Wtedy wartość systemu aktywnego (zabezpieczanego) wynosi w chwili t:

$$0 \le v_t \le v_o.$$

Niech decyzję systemu określa zmienna:

$$Y_{ijk} = \begin{cases} 1, & \text{jeśli } B_k \text{ zabezpiecza obiekt } S_j \text{ przed zagrożeniem } Z_i, \\ 0, & \text{w przeciwnym wypadku} \end{cases}$$

czyli określa się „potencjał" poszczególnych środków zabezpieczenia do poszczególnych obiektów przed możliwymi i dopuszczalnymi zagrożeniami, przy czym:

$$\sum_{k=1}^{K} Y_{ijk} \le M$$

czyli każdy obiekt jest zabezpieczany (w szczególności za wyjątkiem tych obiektów, których ochrona jest nieopłacalna). Wtedy funkcja wartości w chwili t ma postać:

$$v_t(x,y) = \sum_{j=1}^{M} \left(v_{jo} - \sum_{i=1}^{N} \sum_{k=1}^{K} f_{ijk} x_{ij} y_{ijk} \right)$$

przy czym zakładamy, że decyzja otoczenia $x = \langle x_{ij} : i = 1,2,...,N, j = 1,2,...,M \rangle$ jest systemowi znana.

Strategia obrony systemu:

System dokonuje takiego „przydziału" środków zabezpieczenia do ochrony poszczególnych elementów przed przewidywanymi zagrożeniami, który maksymalizuje wartość systemu w chwili t, czyli:

$$\max_{y \in Y} V_t(\hat{x}, y) = V_t(\hat{x}, y^*)$$

gdzie Y – zbiór dopuszczalnych decyzji systemu,

y^* - optymalna strategia obrony systemu aktywnego przed zagrożeniami ze strony otoczenia.

Załóżmy, że dana jest uogólniona funkcja wartości systemu taka, że sytuacja zagrożenia może być sprawdzona do **modelu sytuacji konfliktowej** w postaci **gry dwuosobowej:** $\Gamma = \langle S, O; Y, X, F(x,y) \rangle$ gdzie F(x,y) jest funkcją „wpłaty", czyli:

$$\max_{y \in Y} \min_{x \in X} F(x,y)$$

System maksymalizuje swoją wartość (wartość zasobów znajdujących się w jego elementach), otoczenia zaś minimalizuje ją (czyli maksymalizuje straty systemu).

Sytuację konfliktową określa zatem następująca struktura:

$$SYT \equiv \langle S, O, R; Z, B \rangle$$

oraz gra:

$$\Gamma = \langle S, O; X, Y; F(x,y), x \in X, y \in Y \rangle .$$

Model walki

Z ogólnej analizy podstawowych modeli walki Lanchestera wynika, że stopień, w jakim strony walczące prowadzą „ogień punktowy" lub „ogień powierzchniowy" zależy od wiedzy – informacji o sytuacji na polu walki. Im pełniejsza jest wiedza strony, tym bardziej jego działania są zgodne z prawami ognia punktowego. Względna efektywność walki przez obie strony jest bezpośrednio związana ze stanem jego wiedzy (stopniem poinformowania).

Powyższe zależności można przedstawić w postaci modeli walki Helmbolda:

$$\frac{dx}{dt} = -a(t)\left(\frac{x}{y}\right)^{1-W_y} \cdot y$$

$$\frac{dy}{dt} = -b(t)\left(\frac{y}{x}\right)^{1-W_x} \cdot x$$

w którym można wyróżnić przypadki:

a) przypadek kompletnej wiedzy, odpowiadającej „ogniowi punktowemu" $(W_x = 1,\ W_y = 1)$,

b) przypadek niepełnej wiedzy, odpowiadający „ogniowi powierzchniowemu" $(W_x = W_y = 0{,}5)$,

c) przypadek błędnej informacji, odpowiadający działaniu gorszemu niż „ogień powierzchniowy" $(W_x \langle 0{,}5\ ,\ W_y \langle 0{,}5)$,

d) przypadek całkowicie błędnej informacji $(W_x = W_y - 0{,}5)$, co może prowadzić do „samozniszczenia" $(\dot{x} = -ax\ ,\ \dot{y} = -by)$.

Model walki cybernetycznej

Zakłada się, że zjawisko *„cyberwar"* posiada następujące cechy:

(1) misją jest uzyskanie przewagi informacyjnej (przewagi wiedzy nad przeciwnikiem;

(2) przeciwnik jest „niewidzialny", tzn. funkcjonuje on w „strukturze wirtualnej" którą tworzą relacje tworzone *ad hoc* w „przestrzeni cybernetycznej";

(3) terenem działań jest „przestrzeń cybernetyczna" *(cyberspace)*, czyli dowolny obszar megasieci (globalnej sieci teleinformatycznej);

(4) podstawową formą są *„cyberataki"* o wielorakich źródłach i różnorodnych formach (w tym „cyberterrorystyczne");

(5) szczególnej wagi obiektem „cyberataków" jest tzw. krytyczna infrastruktura państwa, jej poszczególne elementy i podsystemy, oraz elementy infrastruktury systemów typu C4ISR;

(6) czynnikiem krytycznym jest czas, w tym zdolność do wykonania cybernetycznych uderzeń uprzedzających prowadzących do dezorganizacji i utraty zdolności sterowania przez podstawowe systemy przeciwnika;

(7) walk cybernetyczna może

- stanowić element każdej operacji militarnej, a także „operacji innej niż wojna";
- mieć ograniczony zasięg (np.dany rejon lub region);
- mieć zasięg nieograniczony, czyli może być prowadzona w dowolnym miejscu i w dowolnym czasie;
- może mieć zasięg globalny, czego skutkiem może być dezorganizacja globalnej sieci informacyjnej.

(8) "cyberwar" wymaga rekonstrukcji paradygmatu bezpieczeństwa i obrony państwa oraz prowadzenia wojny;

(9) nowy paradygmat „wojny cybernetycznej" wymaga odejścia od liniowego postrzegania sytuacji i przyjęcia „sieciowego" myślenia i działania, zakładającego konieczność postrzegania sytuacji jako „sieci nieliniowych sprzężeń zwrotnych";

(10)„walka cybernetyczna" (cyberwar) może w przyszłości stworzyć warunki do osiągnięcia celów wojny (celów politycznych) nie na „tradycyjnym" polu walki z wykorzystaniem energomaterialnych (niszczących) środków, lecz w „przestrzeni cybernetycznej" za pomocą środków informacyjnych skierowanym przeciw systemom (zasobom) informacyjnym.

2.1.3. Scenariusz RAND (The Day After ... in Cyberspace)

ZESTAWIENIE ZDARZEŃ GRY WOJENNEJ RAND

Symulacje gry wojennej zaczynają się od zdemaskowania (ujawnienia) płaszczyzny konfliktów informacyjnych i problemów związanych z nimi. RAND stworzył i zaprezentował grę dla starszych przedstawicieli rządu w 1995 roku zatytułowaną „ *The Day After ... in Cyberspace*"[1]. Zdarzenia informacyjne wykorzystane w grze, w większości przypadków przedstawiają faktycznie zaistniałe przypadki awarii systemów informacyjnych.

Tab. 1 Zestawienie zdarzeń Gry Wojennej RAND[2]

Numer zdarzenia	Typ ataku	Podobne zdarzenie na świecie
Przerwa w zasilaniu w energię elektryczną w Kairze - 11 maja - wyłączenie 90% energii elektrycznej w rejonie Kairu na kilka godzin.	**Bomba logiczna** - Typ „*Konia Trojańskiego*", który może, ale nie musi być wirusem. Składnikiem ich zadań jest uruchomienie przez zaistnienie określonych warunków (prawda / fałsz). Bomby logiczne nie rozprzestrzeniają się: siedzą i czekają.	Szpiegostwo komputerowe - agenci niemieckiego wywiadu uzyskali nielegalny dostęp do wielu komputerów na świecie poprzez sieć NASA SPAN. Włamali się do systemu komputerowego fizycznego laboratorium Europejskiego Laboratorium Fizyki Molekularnej (CERN) w Genewie i załadowali niszczycielskiego „*Konia Trojańskiego*", który niszczy oprogramowanie i rozbili systemy.

[1] *Nazajutrz... w cyberprzestrzeni*

[2] *Źródło: opracowanie własne na podstawie The Day After... in Cyberspace, [w:] www.rand.org/publicatios*

Wyłączenie Publicznej Sieci Telekomunikacyjnej w stanach Kalifornia / Oregon -11 maja – w Publicznej Sieci Telekomunikacyjnej w północnej części Kalifornii i Oregonie doszło do serii masowych awarii.	**Pułapka** (trap door) - ukryty system oprogramowania uruchomiony w celu zmylenia środków zabezpieczających system. Może to być zgodny z technicznym oprogramowaniem pozwalającym intruzowi obejść procedurę logowania lub bezpośredni dostęp do źródła kodu dostępu. Jego istnienie, w przypadku, gdy jest znane osobie nieuprawnionej może być źródłem znaczącego naruszenia bezpieczeństwa.	Legion of Doom Time Bomb -W 1990 roku, kilku członków oddziału Legionu w Atlancie zostało aresztowanych pod zarzutem penetracji i zakłócenia elementów sieci telekomunikacyjnej. Agenci federalni oskarżyli członków legionu o umieszczenie serii zakłócających programów typu „time bomb" w elementach sieci w Denver, Colorado, Atlancie, Georgii oraz New Jersey. Te bomby czasowe zostały zaprojektowane w celu wyłączenia głównych koncentratorów, ale zostały zneutralizowane przez pracowników firmy telefonicznej zanim spowodowały jakiekolwiek zniszczenia. Opierając się na analizach publikacji, autor wierzy, że grupy intruzów elektronicznych zorganizowane i finansowane przez zainteresowanych przeciwników są w stanie przeprowadzić wyszukane zakrojone na szeroką skalę ataki na Publiczne Sieci Telekomunikacyjne (PSN). Ten typ ataków może spowodować znaczne obniżenie możliwości krajowej agencji Bezpieczeństwa Narodowego i Gotowości do Przeciwdziałania Sytuacjom Nadzwyczajnym w dziedzinie telekomunikacji, spowodować znaczne problemy ze zdrowiem i bezpieczeństwem publicznym oraz spowodować poważne wstrząsy ekonomiczne.

Ft. Lewis Mass Dialing Attack - 11 maja - Zablokowanie systemu łączności telefonicznej bazy Fort Lewis (Waszyngton) poprzez zmasowane wybieranie numerów telefonicznych z wykorzystaniem komputerów osobistych	**Przeciążenia informacyjne** (info overload)	Udokumentowane umiejętności naruszycieli - elektroniczni naruszyciele demonstrują zdolności punktom zarządzania usługami, systemom zabezpieczenia usług, systemom międzysiegciowym, usługi modyfikowania danych użytkownika, rozmów wychodzących, modyfikowanie uprawnień przypisanych łączom, wyłączenia bilingu na wybranych łączach, tabele kierowania ruchem i opisy usług. Scott Maverick skompromitował 911 usług w 1992 roku. Został aresztowany za fałszowanie tych systemów w Virginii, Maryland i New Jersey. Maveric wyznał, że jego zamiarem było zarażenie tych 911 komputerów wirusem, żeby je zniszczyć. Znaczna degradacja usług dla 911 systemów jest możliwa, jeśli są one zaatakowane przez elektronicznych naruszycieli.

Wybuch w rafinerii ARAMCO - 13 maja – w największej rafinerii ARAMCO w pobliżu Dhahran (Arabia Saudyjska) dochodzi do katastrofalnej awarii systemu sterowania przepływem, która doprowadziła do wielkiego wybuchu i pożaru.	**Bomba logiczna**	Obwiniony Kevin Poulsen- Kierowana rzekomo z ukrycia w kwietniu 1991 roku próba wtargnięcia w całkowity system komputerowy i telefoniczny. Był to do dnia dzisiejszego najbardziej wszechstronny, skoordynowany atak na Publiczną Siec Telekomunikacyjną. Obwiniony o wszystko z następującej listy zarzutów: skompromitował przepisy prawa wg, których prowadzono dochodzenie; rozpoznał przepisy prawa w prowadzeniu interesów i przepisy dotyczące wykorzystania podsłuchów. Wielokrotnie włamywał się (rzekomo więcej niż 40 razy) do lokalnego nośnika wymiany usług (LEC) zarządzania systemem; zmodyfikował istniejące usługi telefoniczne; dodał nowe usługi telefoniczne (niektóre bez billingu); przekazał rozmowy na inne numery i podwójnie zabezpieczone linie telefoniczne; włamał się do systemu obsługi i testowania LEC, żeby elektronicznie monitorować rozmowy telefoniczne; włamał się do bazy danych LEC i uzyskał numery telefonów, adresy, nazwiska klientów oraz inne dyskretne informacje; włamał się fizycznie do biur LEC i skradł wyposażenie, oprogramowanie, znaczki identyfikacyjne i inne materiały; sprzedał dyskretne dane uzyskane z bazy danych LEC i nielegalnie ustanowił lub zmodyfikował usługi telefoniczne dla innych; wyrobił fałszywy identyfikator, włączając znaczek identyfikacyjny firmy telefonicznej i prawa jazdy; włamał się do innych systemów komputerowych dla uzyskania korzyści, włączając Wydział Komunikacji Kaliforni, biura kredytowe i sieć komputerową Lotnictwa Wojskowego; nielegalnie posiadał dokumenty niejawne (zarzut za który został uznany niewinnym); prał pieniądze. Chociaż Poulsen nie atakował Publicznych Sieci Telekomunikacyjnych to manipulował nimi dla własnych celów oraz dla własnych korzyści.

Katastrofa szybkiego pociągu pasażerskiego - 14 maja - w pobliżu Laurel, Maryland, nowy superszybki pociąg pasażerski, jadąc z prędkością 300 km/h uderzył w znajdujący się na niewłaściwym torze pociąg towarowy, zginęło ponad 60 pasażerów i załoga, rannych zostało 120 osób.	**Bomba logiczna**	Wypadek kolejowy w Arizonie w 1995 roku - Badanie wraku pociągu w odizolowanej części pustyni Arizona wykazało, że w urządzeniu komputerowym monitorującym komputerowy system bezpieczeństwa wystąpiło krótkie zwarcie. System był zainstalowany aby ostrzegać o tym, że tory są wolne, ale zawiódł, najwidoczniej na skutek czyjejś ingerencji.

Bank Anglii - 16 maja - Scotland Yard poinformował Premiera Anglii, że w Banku Anglii wykryto trzy różne nowoczesne urządzenia wykrywające (detektory) w systemie transferu głównych funduszy w związku z czym przedstawiciele banku obawiali się, że ktoś nieuprawniony mógł się włączyć w system transferów bankowych.	**Detektory** - programy komputerowe zaprojektowane dla analizy sieci łączności. Diagnozują one problem i pomagają administratorowi sieci w ich rejestracji. W niektórych przypadkach są one pisane w ten sposób, że administratorzy systemów nie są świadomi faktu, iż ktoś poza nimi ingeruje w system zbioru informacji sieci takie jak hasła, wprowadzone dane oraz wsłuchuje się w transmisje telekomunikacyjne. Detektory mogą być pisane w celu wyszukiwania informacji, które pozwolą użytkownikowi ukradkiem włączyć się w system oraz/ lub manipulować systemem w okresie późniejszym.	10 milionów dolarów zdefraudowanych z kasy Citibank -34 letni Rosjanin, działając z Saint Petersburga zdołał uzyskać dostęp do kodów dostępu i przelać 10 min dolarów z kont Citibank w Argentynie i Indonezji. Łączymy ten przypadek ze zdarzeniem na Uniwersytecie Kalifornia w 1994 roku, gdzie z wykorzystaniem nieuprawnionego programu zgromadzono dziesiątki tysięcy nazwisk posiadaczy kont i haseł poprzez detektor umieszczony w Internecie.

Przekłamania na wykazie tymczasowej dyslokacji sił - 20 maja - Departament Obrony wykrył przekłamania danych na wykazie tymczasowej dyslokacji sił	**Wirus**	Płatni informatorzy - Przedstawiciele agencji National Communications System (NCS) twierdzą, że istnieje wiele dowodów na to, że osoby wtajemniczone sprzedają poufne informacje agentom informacyjnym, szpiegom przemysłowym, organizacjom przestępczym oraz służbom wywiadowczym. Osoby wtajemniczone, posiadające pełny dostęp do informacji dostarczają dane o niejawnych numerach telefonów, zapisy rozmów, poufne relacje oraz inne dane osobowe. FBI informuje, że organizacje przestępcze uzyskały dostęp do rejestrów Narodowego Centrum Informacji o Przestępstwach, wykorzystując do tego celu skompromitowanych pracowników tego centrum. W grudniu 1991 roku 18 pracowników Social Security Administration zostało oskarżonych o sprzedaż poufnych informacji.
Niesprawność bankomatu - bankomaty dwóch największych sieci bankowych w Georgii	**Bomba logiczna**	Straty w wyniku defektów oprogramowania wyniosły 70 mln $ - 70 mln rządowych $ strat spowodowanych opłaceniem przez Administrację Finansowania Opieki Zdrowotnej z powodu niesprawności oprogramowania w wyniku skarg pacjentów. Pieniądze zostały wypłacone za wykonane usługi; niemniej jednak nie wszyscy pacjenci zostali wybrani. Największej organizacji wypłacono 19 min $.

Katastrofa samolotu pasażerskiego - 22 maja pilot nowego samolotu pasażerskiego AB-340 linii CONTINENTAL wykonując końcowe zbliżanie do Międzynarodowego Lotniska 0'Hare zameldował, że w wyniku masowych niesprawności przyrządów pokładowych samolot wykonuje niekontrolowany lot. Doszło do katastrofy w wyniku, której zginęło 30 osób a 100 innych zostało rannych. Na podstawie meldunku eksperci wywnioskowali, że oprogramowanie kontroli lotu samolotów AB-340 oraz 330 może być zainfekowane przez wy rafinowaną bombę logiczną w wyniku czego Federal Aviation Administration zawiesiła loty wszystkich tego typu samolotów.	**Bomba logiczna**	Niezadowolony pracownik firmy dostarczającej systemy obronne (Defense Contractor) - W sierpniu 1992 roku administrator systemów komputerowych firmy dostarczającej systemy obronne dowiedział się o nierozstrzygniętym projekcie. Pracownik umieścił złośliwy kod, żeby go aktywować po swoim wyjeździe, spodziewając się, że firma wezwie go ponownie dla rekonstrukcji bazy danych po spracowaniu bomby logicznej. Jego próba została wykryta jeszcze przed jego wyjazdem a on sam został oskarżony. Jeśli ten złośliwy kod by spracował, bardzo ważne dane dotyczące rozbudowy wojskowych systemów rakietowych zostałyby zniszczone a ich odtworzenie trwałoby wiele miesięcy.

Przejęcie Saudi News - 23 maja główne rządowe sieci informacyjne Arabii Saudyjskiej zostały nagle zastąpione przez twarz przywódcy Rady CIRD, który wezwał obywateli Arabii Saudyjskiej do poparcia wysiłków w celu pokojowego przekształcenia Królestwa Saudyjskiego w wolne i demokratyczne państwo Islamu. Spreparowany sygnał doprowadził do zakrojonych na szeroką skalę demonstracji przeciwko monarchii Saudyjskiej.	**Spamming**- (wykorzystując technologię) przejęcie transmisji i zastąpienie pokazywanego obrazu swoim własnym programem.	Wykazane technologie.

Niesprawność Saudyjskiej PSN (Publicznej Sieci Telekomunikacyjnej) - 23 maja Sieć PSN w Arabii Saudyjskiej zaczyna się psuć najprawdopodobniej wskutek nieautoryzowanych zmian w systemie spowodowanych „trap door" - pułapkami.	**Bomba logiczna**	Jak w przypadku 4 (Kevin Poulsen Pleads Guilty)
Ataki w ramach Wojny Informacyjnej (Information Warfare Attacks) przeciwko bazom Amerykańskim - 23 maja - Sekretarz Obrony został poinformowany, że pełno wymiarowy atak informacyjny nieznanego pochodzenia prowadzony jest przeciwko prawie wszystkim amerykańskim bazom wojskowym w USA	**Próby wielokanałowe**	Rezultaty „Czerwonego Zespołu" Agencji Obrony Systemów Informacyjnych - Defense Information Systems Agency (DISA) Red Team Results. Zespół spróbował uzyskać dostęp do 9000 komputerów w całym Departamencie Obrony. Udało się zpowodzeniem włamać do 88% (ponad 7900) z nich. Zostawili znaki swoich wykroczeń, ale dotychczas zaledwie ponad 300 znielegalnych wejść zostało wykrytych. Administratorzy sieci w Centrum Wojny Informacyjnej Sił Powietrznych twierdzą, że są w stanie złamać 70% haseł dostępu do swoich sieci UNIX zwykorzystaniem narzędzi przypominających te, które są używane przez hackerów internetowych.

i Europie, zaangażowanym w dyslokację w Arabii Saudyjskiej.		
Niesprawność wspólnej stacji radiolokacyjnej systemu obserwacji okrężnej oraz obserwacji atakowanego celu - 24 maja - kilka stacji radiolokacyjnych systemu JSTARS wspólnej obserwacji okrężnej oraz obserwacji atakowanego celu samolotów działających w regionie Zatoki Perskiej odniosło wrażenie jakoby były nękane przez komputerowego robaka spuszczonego przez jakieś nieznane źródło zewnętrzne.	**Worm** - ***Mikrob*** - Program komputerowy który zjada pamięć i zasoby komputera, efektywnie czyniąc go bezużytecznym	Elektroniczne intruzy- Przybywa przykładów wykorzystania technik elektronicznych intruzów przez szpiegów przemysłowych. W poddanych sprawdzeniu 150 technicznych firmach badawczo rozwojowych, 48% twierdzi, że były celem kradzieży tajemnic handlowych. Łączymy tę informację z przypadkiem Kevina Mitnicka, który w 1989 roku został aresztowany o oskarżony o kradzież wartości ponad 1 min $ materiałów kodowych z Digital Eguipment Corporation (DEC), przerabiając je na pułapki („trap doors"), następnie próbował skopiować je ponownie do komputerów DEC. JSTARS jest programem w dużym stopniu uzależnionym od oprogramowania i to sprawia, że mógł on być podatny na tego typu wtargnięcia (ingerencje).

Wyłączenie telefonów w District Columbia / Baltimore - 24 maja -cała sieć telefoniczna w regionie Waszyngton / Baltimore, włączając lokalny system telefonów komórkowych, uległa awarii.	**Bomba logiczna**	Wyłączenia innych systemów telefonicznych - W 1991 roku prawie całkowicie wyłączono usługi telefoniczne w rejonie Waszyngton/ Baltimore w wyniku błędu kodowania w nowym oprogramowaniu dalekosiężnym AT&T. Obsługa autostrady kopiąc dziurę pod filar przerwała rozmowy w relacji wybrzeże - wybrzeże z powodu przecięcia przewodu światłowodowego MCI. Podobny przypadek w New Jersey przerwał 60% rozmów do i z Manhattan na 8 godzin. W tym przypadku Giełda Handlowa i Towarowa Nowego Yorku musiały zawiesić operacje. Ponadto systemy głosowe i radiolokacyjne używane do kontroli ruchu lotniczego ze stanowisk w Nowym Jorku, Waszyngtonie i Bostonie były obezwładnione przez 5 godzin.

Fluktuacja na Giełdzie w Chicago - 24 maja - Giełda Towarowa Chicago doznała pewnego rodzaju najburzliwszej fluktuacji w historii. Istnieje powszechne podejrzenie, że Giełda stała się obiektem potężnej manipulacji elektronicznej dokonanej przez nieznane ugrupowanie.	**Bomba logiczna**	Warianty wyłączeń - Podobne przypadki podane wcześniej

Przejęcie wiadomości CBS -24 maja - wieczorne wiadomości CBS zostały przerwane na 7 minut przez „Aktywne Skrzydło Komitetu dla Pokoju Planetarnego (CPP)". Podczas przejęcia video, rzecznik CPP, dobrze znana i wysoko ceniona osobowość mediów, wezwał do powszechnego obywatelskiego nieposłuszeństwa dla rozbicia administracji, która „straciła kontakt z wewnętrzną i międzynarodowa rzeczywistością".	**Spoofing** - elektroniczna zmiana wyglądu lub słów dla przekazania sensu (znaczenia) innego niż zamierzony przez obiekt filmowany lub fotografowany.	Przedstawione technologie.

W grze założono, że zaistniałe zdarzenia są wynikiem nieprzyjaznych działań. Scenariusz postuluje ataki informacyjne odrodzonego Iranu przeciwko Stanom Zjednoczonym i ich sojusznikom w roku 2000. Dostojnicy uczestniczący w grze byli zobligowani do sformułowania narodowej polityki bezpieczeństwa dla przeciwdziałania nowym formom wojny w postaci rekomendacji dla Prezydenta. Wróg zmierzał do trzech głównych celów w grze RAND.

1. Rozpoczęcie wielokanałowych i urozmaiconych ataków informacyjnych przeciwko licznym obiektom USA i ich sojuszników z zamiarem wywarcia międzynarodowej presji politycznej i podważenia zaufania do możliwości rządu w opanowaniu rozwijającego się kryzysu.
2. Wysiłki wymierzone w infrastrukturę i military centres of gravity w celu zakłócenia zdolności koalicji do walki.
3. Wykorzystano teatr konwencjonalnych operacji wojskowych dla odwrócenia uwagi decydentów narodowych od operacji informacyjnych prowadzonych przeciwko Stanom Zjednoczonym.

Obiekty i typy ataków informacyjnych.

Tabela ilustruje obiekty i typy ataków informacyjnych użytych przeciwko nim, wykorzystane w grze RAND. Ataki informacyjne wroga zacierają różnice pomiędzy wymaganiami wprowadzenia stanu wyjątkowego a zwiększeniem żądań odnośnie kryzysu bezpieczeństwa narodowego.

Systemy transportowe	Sabotaż dyspozytorni kolejowych powoduje zderzenia pociągów. Sabotaż oprogramowania samolotów komercyjnych powoduje katastrofy lotnicze.
Systemy telekomunikacyjne	Zakłócenia w pracy publicznych sieci telekomunikacyjnych w Kaliforni, Oregon, Waszyngtonie i Arabii Saudyjskiej oraz sojuszników USA. Monitorowanie, ingerencja i kradzieże numerów abonentów komórkowych.
Źródła energii	Sabotaż komputerów rafinerii w Arabii Saudyjskiej doprowadza do wybuchu i pożaru.
Systemy finansowe	Bank Anglii wykrywa obcy program zaprojektowany do sabotowania transferu funduszy. Spowodowana programem komputerowym awaria bankomatu w banku Georgia wpływa na sytuację w innych bankach amerykańskich. CNN informuje, że Iran wynajął hackerów dla zaatakowania zachodnich gospodarek, powodując gwałtowne spadki na amerykańskiej giełdzie.
Siły Zbrojne	Zakłócenia w usługach telefonicznych kluczowych baz armii amerykańskiej. Wirus zniekształca dane na wykazie tymczasowej dyslokacji sił (TPFDL) powodując znaczne trudności w dyslokacji amerykańskich sił.
Systemy polityczne	Grupy szczególnych zainteresowań i inne organizacje nie rządowe rozpoczynają doniosłą kampanię propagandową przeciwko ludności amerykańskiej. Transmisje wystąpień przywódców politycznych sojuszników amerykańskich zasiały niezgodę pomiędzy członkami koalicji. Demonstracje organizowane dla podkopania wewnętrznego i sojuszniczego poparcia amerykańskich celów narodowych.

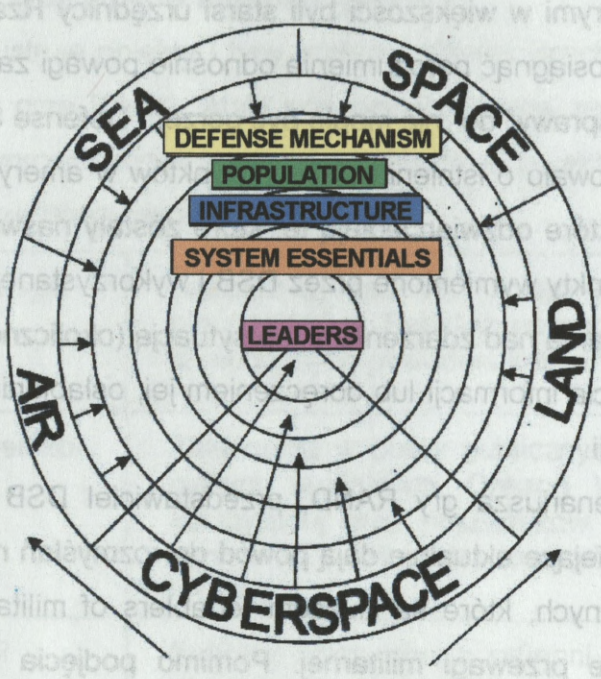
Gracze byli źle przygotowani do nowych wymiarów wojny i nie byli w stanie wspólnie ocenić co się wydarzyło, ani jak się przed tym bronić. Trudno było wypracować definitywne rekomendacje a tradycyjne wojskowe reagowanie na nagle zmieniające się wydarzenia i nietradycyjne ataki nie były efektywne.

Uczestnicy gry, którymi w większości byli starsi urzędnicy Rządu i Departamentu Obrony nie zdołali osiągnąć porozumienia odnośnie powagi zagrożenia z ich ocenami typu od „nie ma sprawy" do „nie mogło być gorzej". Defense Science Board (DSB) Pentagonu zameldowało o istnieniu słabych punktów w amerykańskiej infrastrukturze informacyjnej, które odzwierciedlają te, które zostały naświetlone w grze wojennej RAND. Słabe punkty wymienione przez DSB i wykorzystane w grze RAND obejmują przejęcie panowania nad zdarzeniami lub sytuacją (okolicznościami), zmylenie, manipulowanie treścią informacji lub doręczeniem jej, osłabienie lub zagubienie (zniszczenie) informacji.

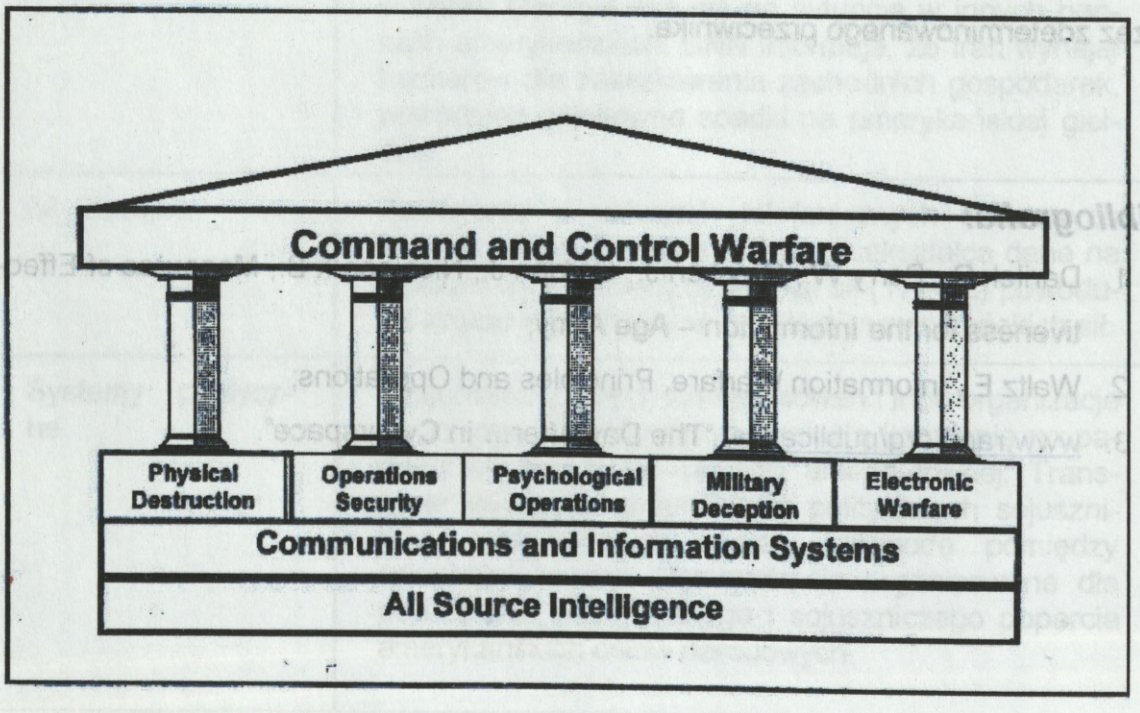
Nawiązując do scenariusza gry RAND, przedstawiciel DSB stwierdził, że działania i możliwości istniejące aktualnie dają powód do rozmyślań nad integralnością systemów informacyjnych, które są kluczem (enablers of military superiority) umożliwiającym uzyskanie przewagi militarnej. Pomimo podjęcia ograniczonych działań dla wykrycia i przeciwdziałania niezorganizowanym zagrożeniom przeciw systemom informacyjnym USA, brakuje narodowych, skoordynowanych możliwości wykrycia, a znacznie bardziej, przeciwdziałania strukturalnym atakom informacyjnym przez zdeterminowanego przeciwnika.

Bibliografia:

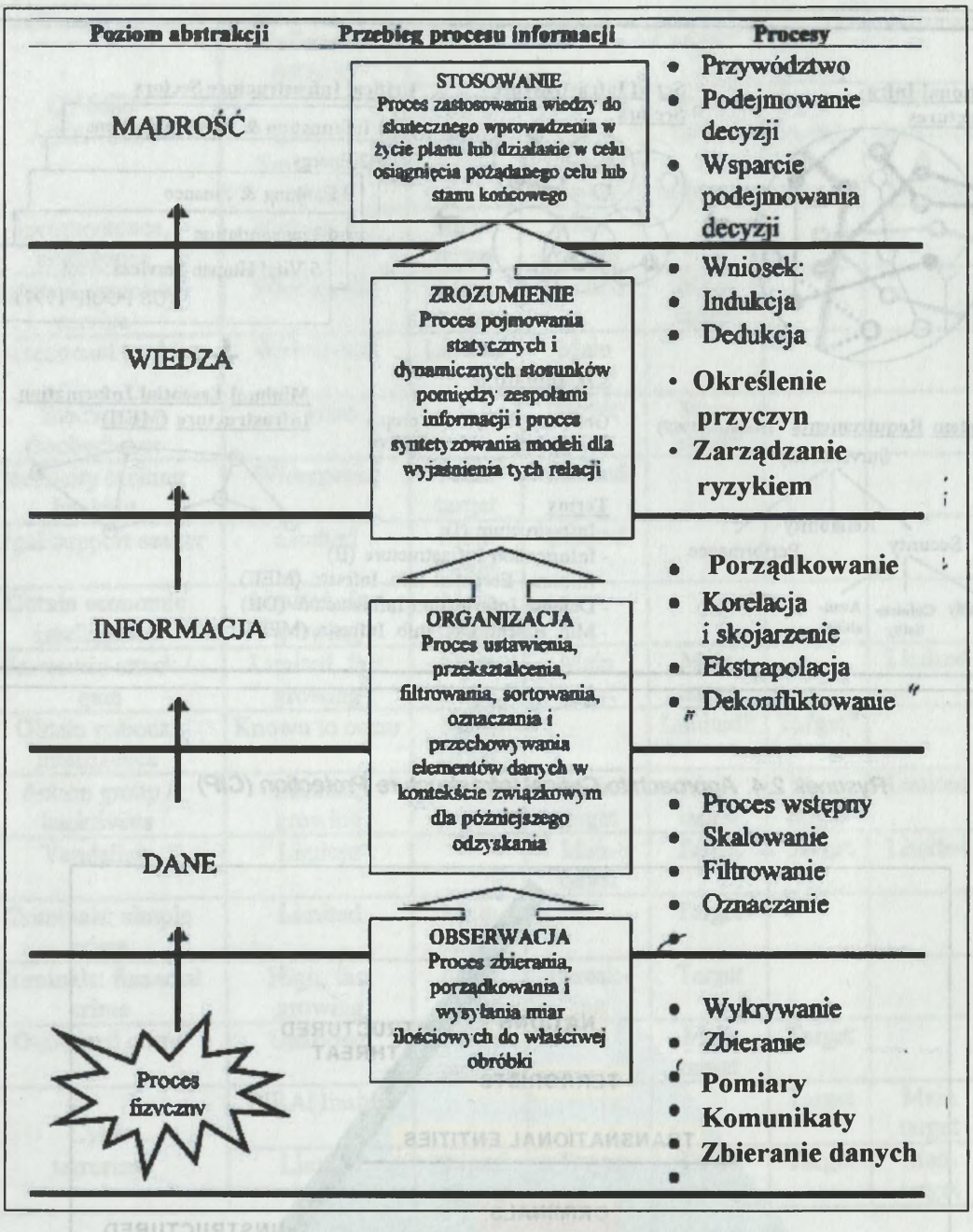
1. Darilek R., Perry W., Gracken J., Gordon J., Nichiporuk B., Measures of Effectiveness for the Information – Age Army;
2. Waltz E., Information Warfare, Principles and Operations;
3. www.rand.org/publicatios, "The Day After... in Cyberspace".



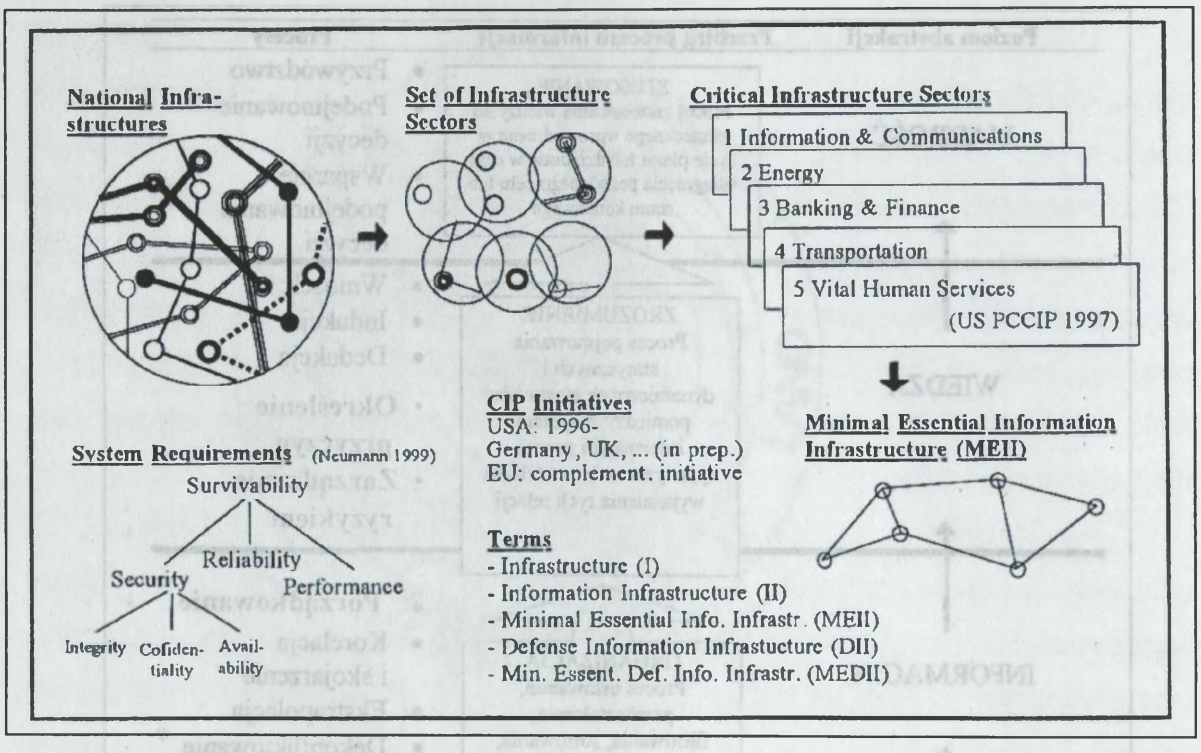
Rysunek 2.1. Model "pięciu wymiarów" walki Wardena.



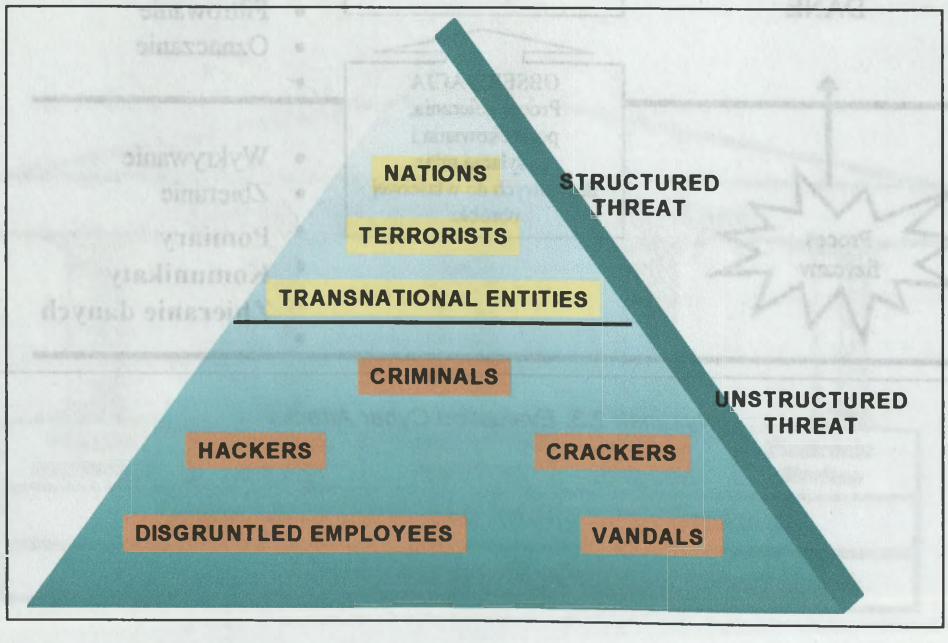
Rysunek 2.2 The five "Pillars" of Command and Control Warfare.



Rysunek 2.3. Evaluation Cyber Attacks



Rysunek 2.4. Approach to Critical Infrastructure Protection (CIP)



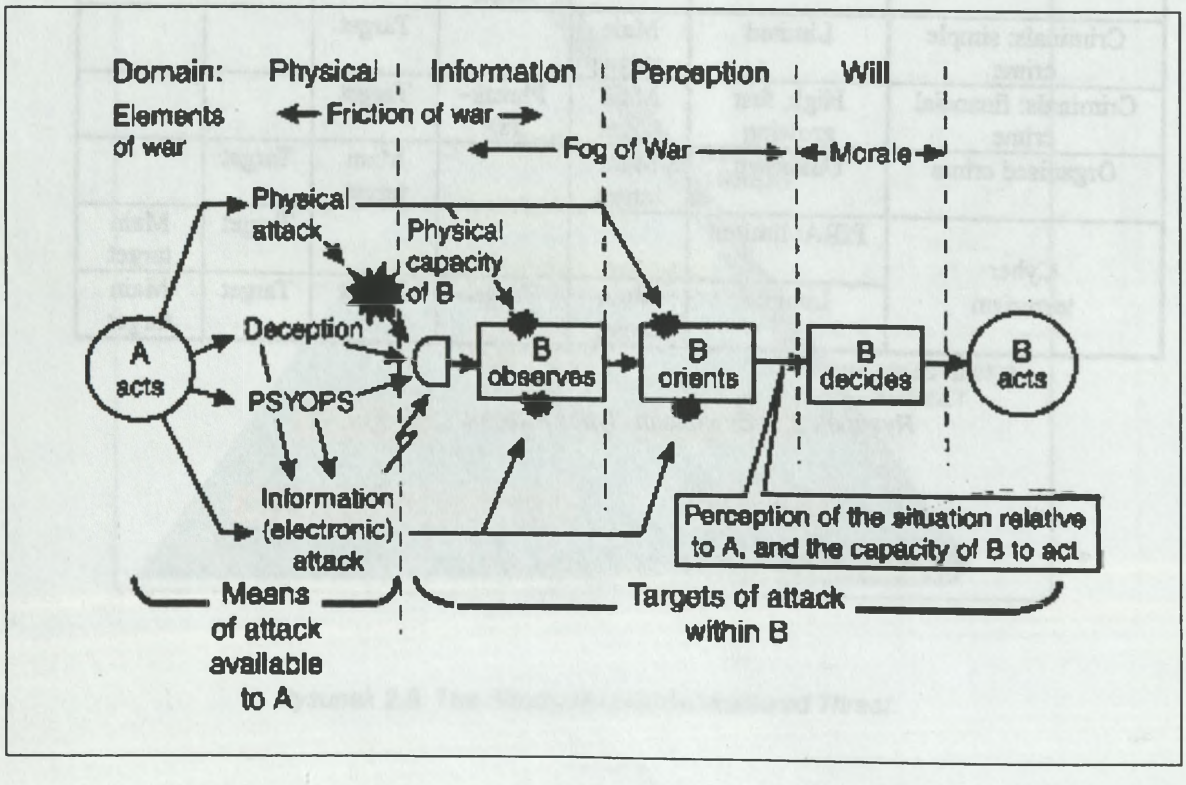
Rysunek 2.5. The Structured and Unstructured Threat.

CYBER ATTACKS	Validated Attacks (Status September 1999)	Targets				
		Infor-mation	Systems & Small Networks	Organi-sation & Industry	Govern-ment	Infra-structure & Society
Incompetence, negligence	Widespread	Main target	Main target			
Internal denial-of-service	Widespread	Main target	Limited	Main target		
Recreational hacking	Widespread	Limited	Main target			
Electronic disobedience	Limited		Target	Main Target		
Publicity seeking hacking	Widespread	Main target	Limited			
Legal support seeker	Limited	Main target	Limited			
Obtain economic intelligence	Limited, fast growing	Main target				
Economic attack / gain	Limited, fast growing	Main target	Main target	Main target		Limited
Obtain national intelligence	Known to occur	Main target		Limited?	Target?	
Action group / hacktivists	Limited, growing	Limited	Main target	Main target	Main target	Limited
Vandalism	Limited		Main target	Target	Target	Limited
Criminals: simple crime	Limited	Main target		Target		
Criminals: financial crime	High, fast growing	Main target	Phreak-ing	Target		
Organised crime	Unknown	Main target		Main target	Target	
Cyber terrorism	PIRA: limited				Target	Main target
	Limited	Main target	Target	Target	Target	Main target

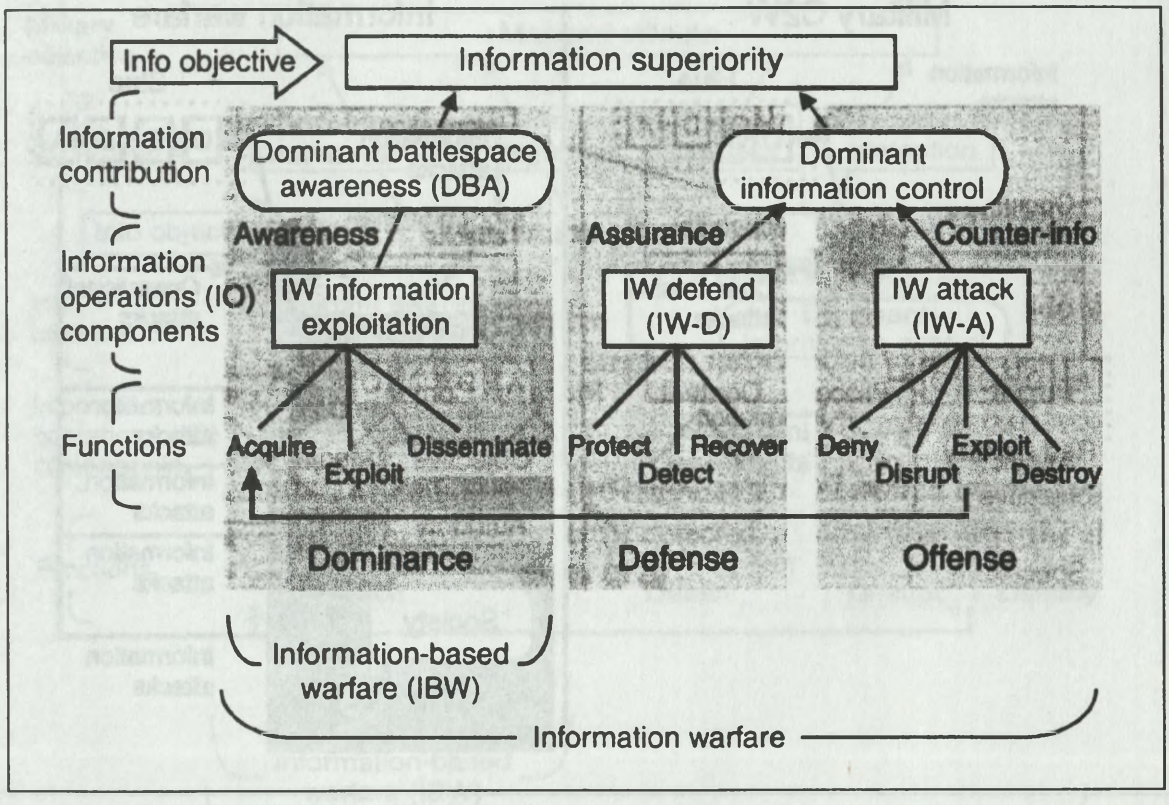
Rysunek 2.6. Evaluation Cyber Attacks.

		Guerrilla Wars		
		High-tech	**Low-tech**	
Economic Based Wars	**Physical conflict**	1. Military C2W . high intensity battle space . economic pressure & power . precision targeting . stealth: physical . C4I technology	3. Guerrilla warfare . low intensity battlespace . ruthlessness . random targeting . stealth: natural environment . human networks (as technology)	**Terrorism**
	Abstract conflict	2. NetWar, CyberWar . Cyberspace conflict . knowledge as power . information base targeting . stealth: using ICT . global networks (as technology)	4. Ideological warfare, conflict and power . mass/society targeting . stealth: ideological . ideological human networks	
		Cultural Wars		

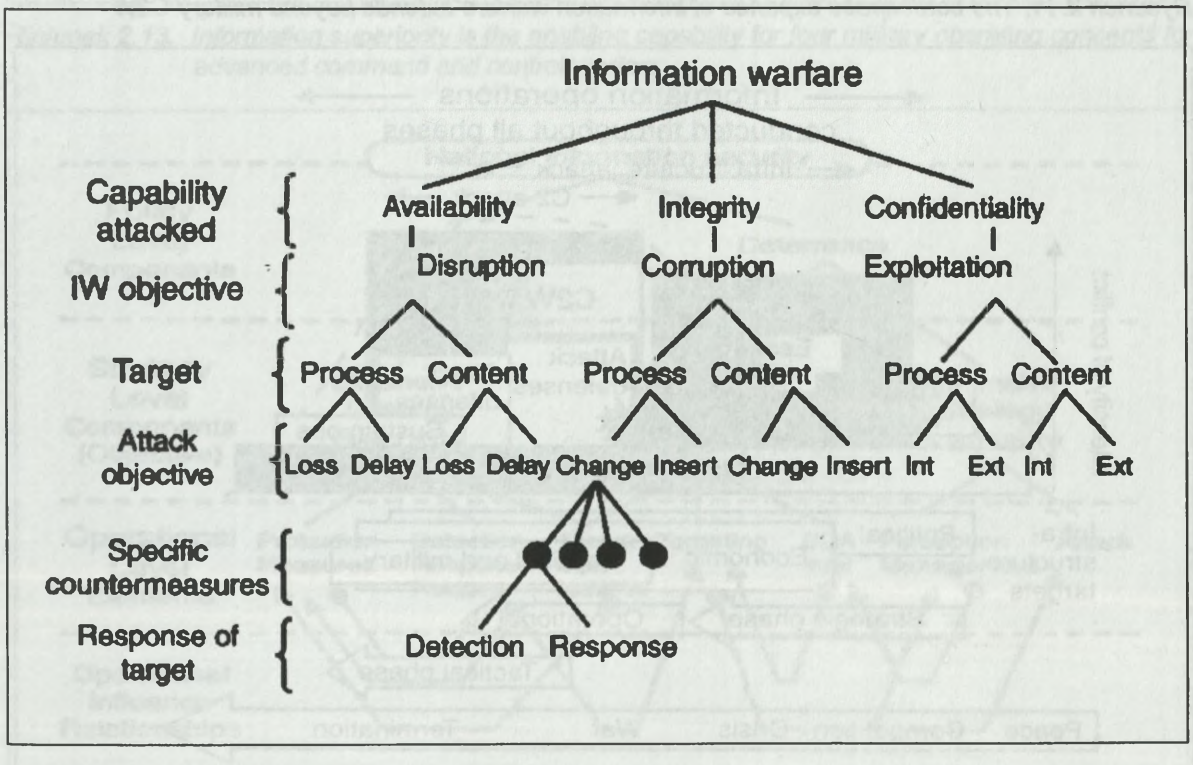
Rysunek 2.7. Typology of four conflict types (Walz, note 19).



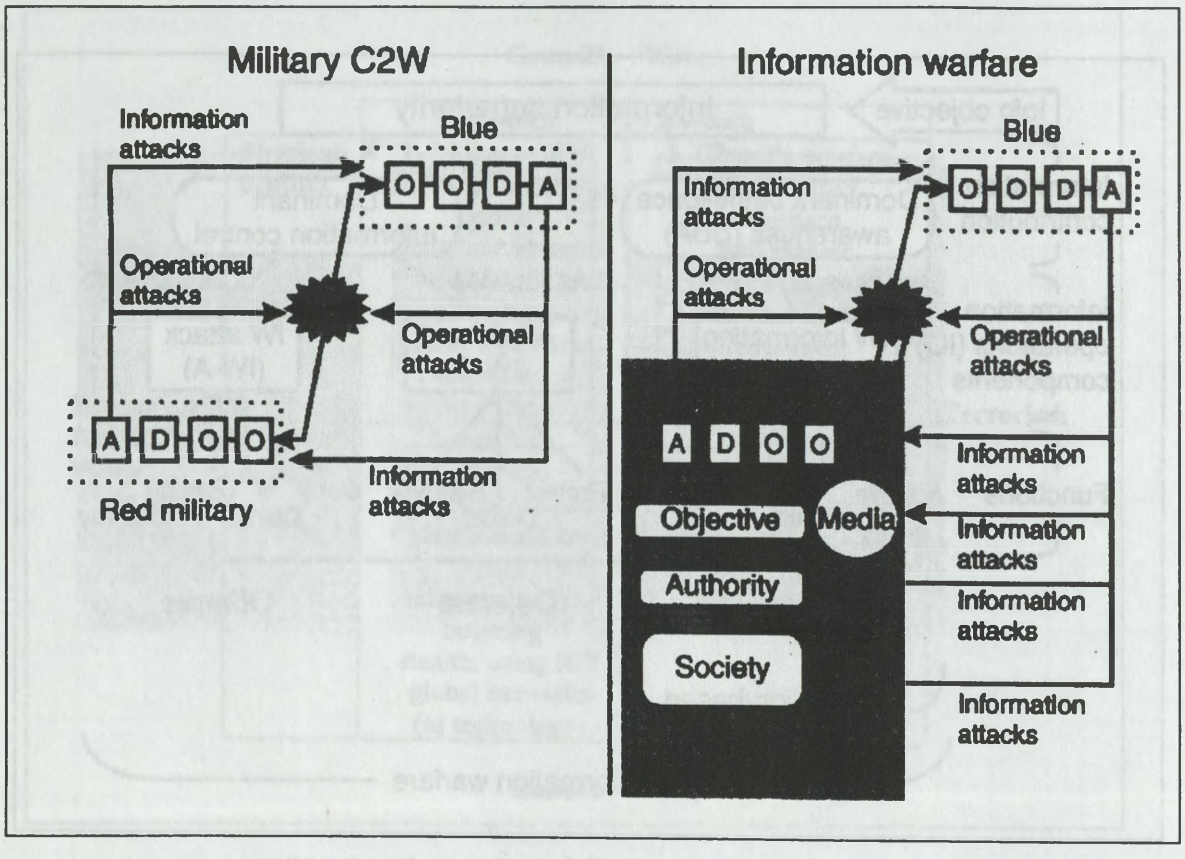
Rys. 2.8. A basic model of the information processes in a conflict between attacker A and defender B.



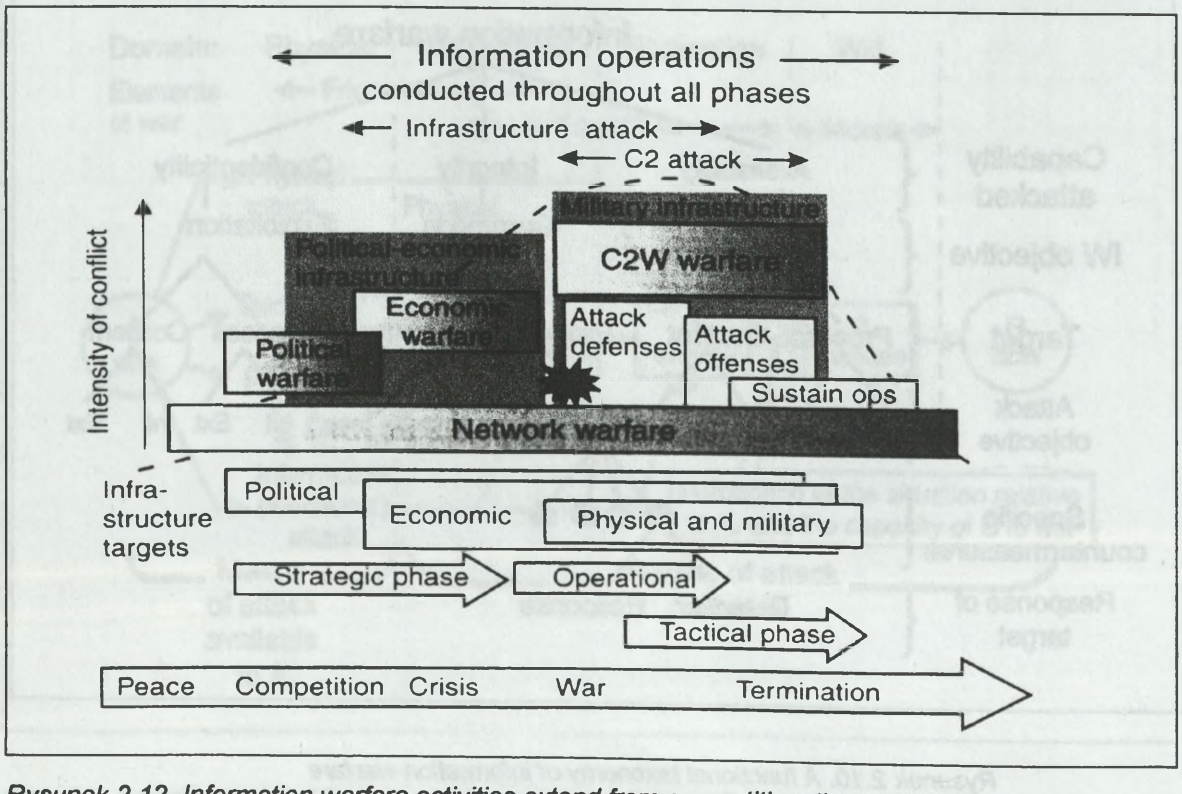
Rysunek 2.9. The components and goal of information warfare operations



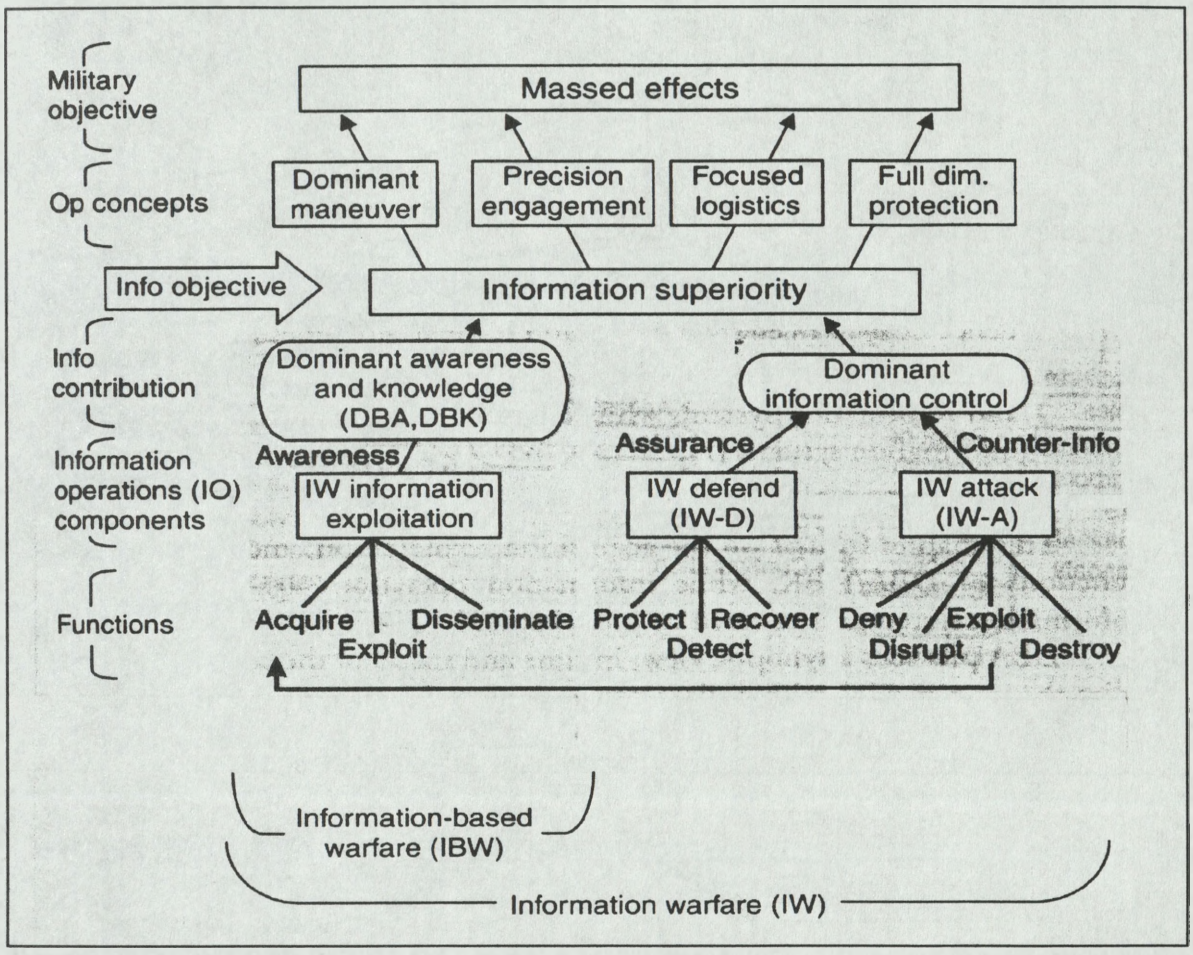
Rysunek 2.10. A functional taxonomy of information warfare



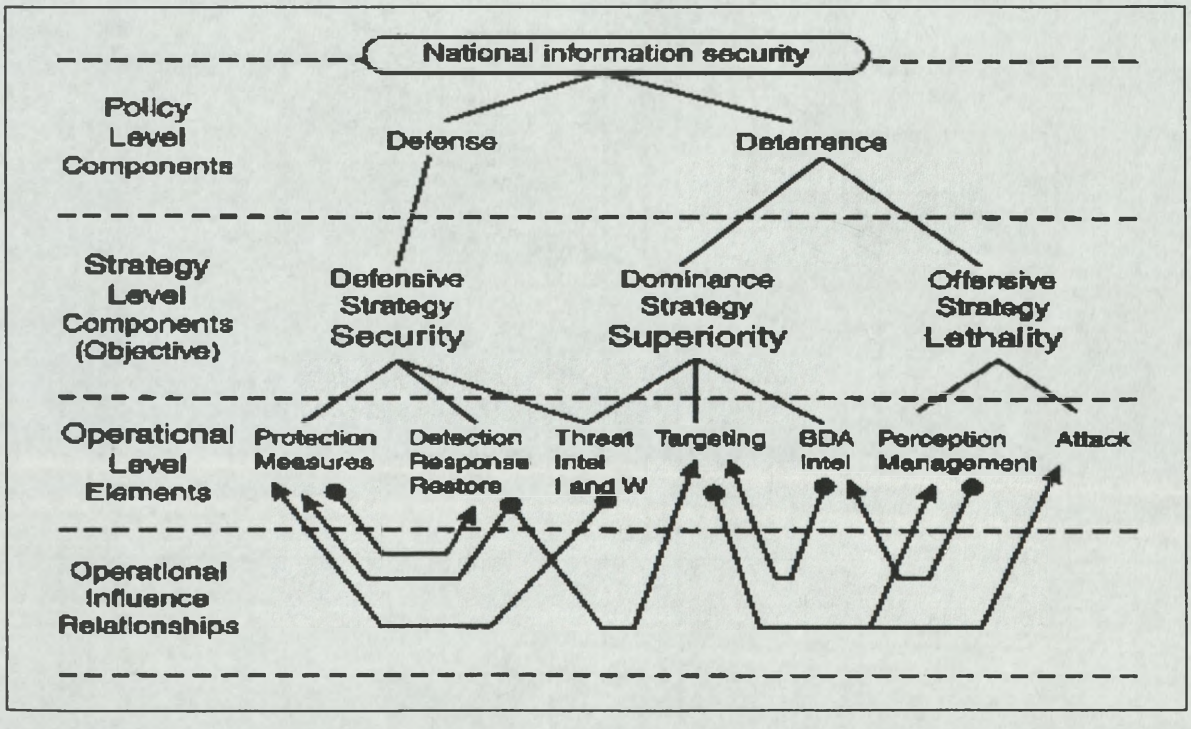
Rysunek 2.11. The battlespace expanse of information warfare extends beyond military C2W



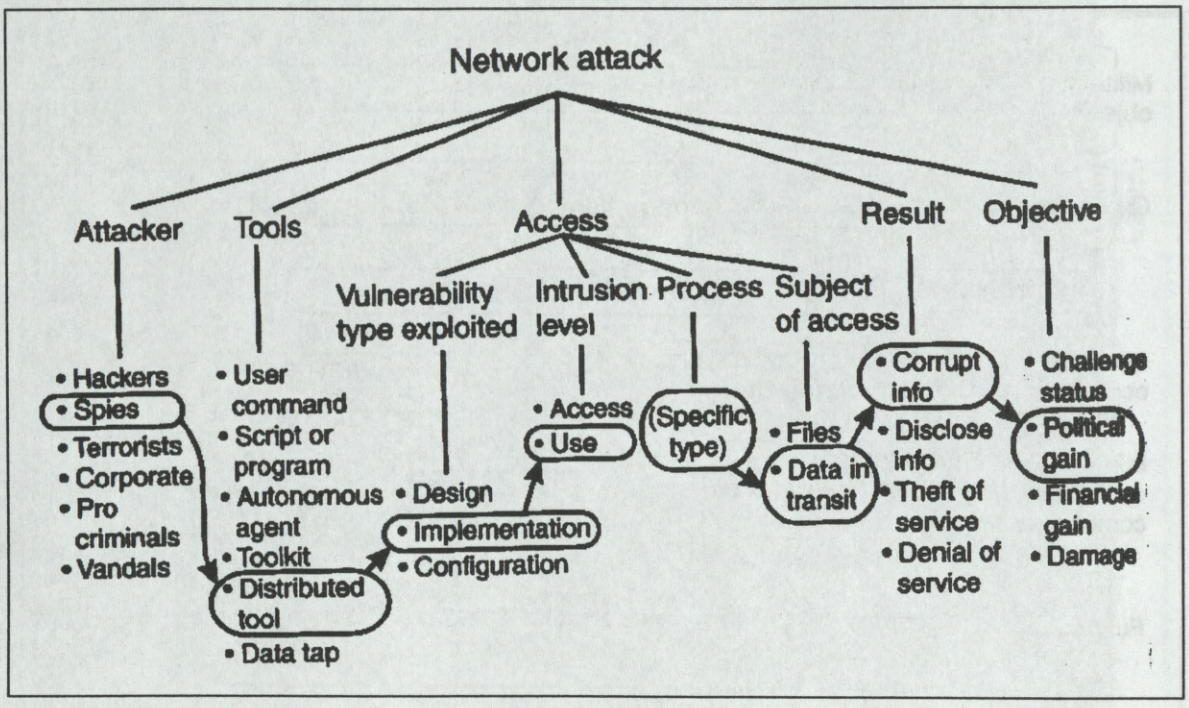
Rysunek 2.12. Information warfare activities extend from competition, through conflict, to war.



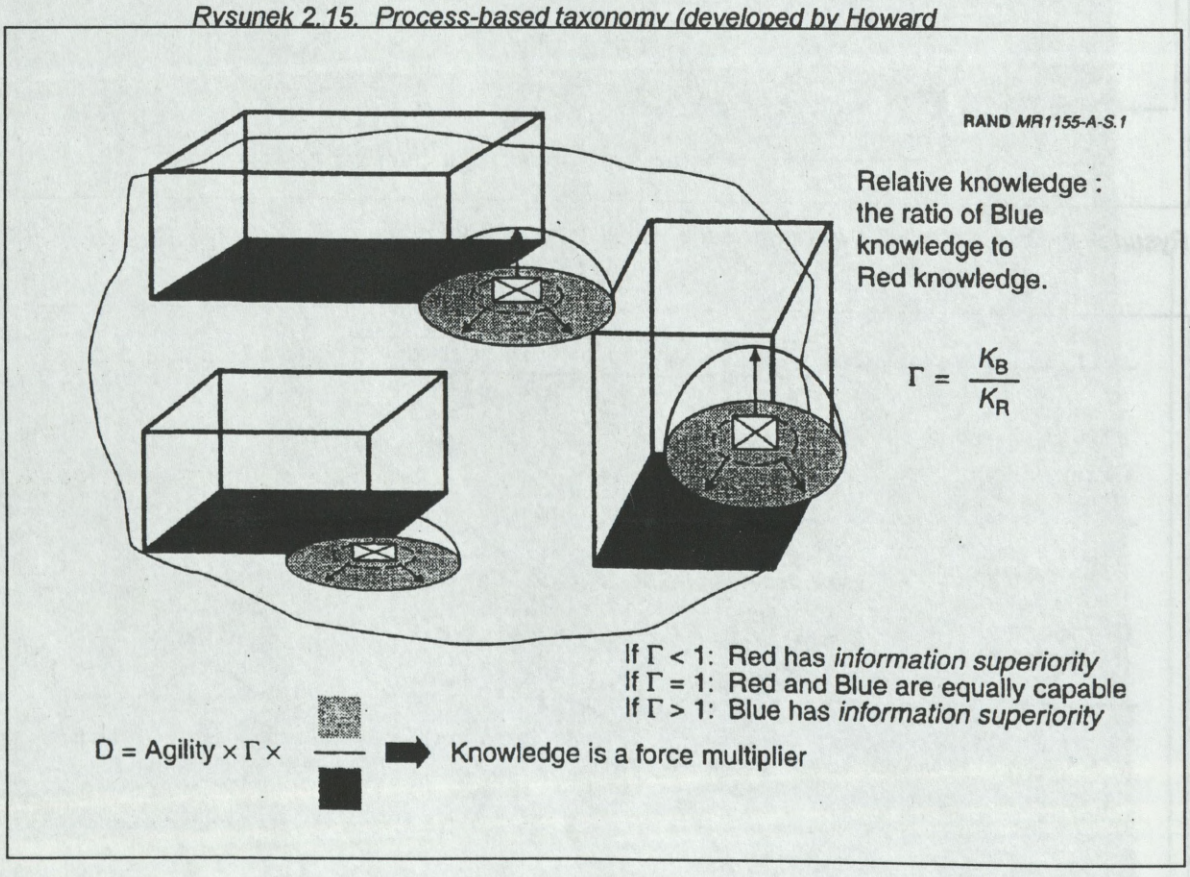
Rysunek 2.13. Information superiority is the enabling capability for four military operating concepts for advanced command and control warfare



Rysunek 2.14. Fundamental hierarchy and components of a national information security strategy.



Rysunek 2.15. Process-based taxonomy (developed by Howard



Rysunek 2.16. The Effect of Knowledg.

2.2. ZAŁOŻENIA OGÓLNE DO SCENARIUSZY ZAGROŻEŃ

Zarówno w środowiskach cywilnych, jak i wojskowych[1] toczy się obecnie coraz szersza dyskusja nad problemami zagrożeń wynikających z działań w sferze informacyjnej. Wojskowi teoretycy i praktycy pracują nad kolejnymi wersjami koncepcji i doktryn działań w sferze informacyjnej. Opublikowanie przez Stany Zjednoczone militarnej doktryny operacji informacyjnych wielu ekspertów uznało za ważny moment historyczny oznaczający początek wyścigu zbrojeń w sferze działań informacyjnych. Zgodnie z nowym dokumentem (Joint Doctrine for Information Operations JP 3-13) pierwszy raz oficjalnie uznano, iż ofensywne ataki na sieci komputerowe stają się nieodłączną częścią arsenału walki USA, a co jeszcze ciekawsze, arsenał ten może być używany także w czasie pokoju. W rezultacie każdy kraj musi zatroszczyć się o uzyskanie zdolności do prowadzenia ofensywnych i defensywnych operacji informacyjnych. Jeśli tego zaniecha, pozostanie bezbronny. Oficjalne wprowadzenie operacji informacyjnych do doktryny militarnej dokonało się między innymi wobec wyraźnych deklaracji wielu krajów, jak np. Chiny, gotowości wykorzystania tej sfery w walce. Jednocześnie wprowadzenie tej sfery do doktryny militarnej oznacza, że rozwinięte zostały możliwości gwarantujące pewność osiągania pożądanych efektów.

Według Roda Starka[2], „...Nie istnieje powszechnie uzgodniona definicja walki informacyjnej. Jest jednak wspólna treść większości spotykanych definicji. Treść ta sprowadza się do tego, że walka informacyjna jest konfliktem, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią. Walka informacyjna obejmuje także fizyczną destrukcję infrastruktury, która wykorzystywana jest przez przeciwnika do działań operacyjnych."

Dla celów opracowania scenariuszy zagrożeń przyjęto, że: **operacje informacyjne** państwa rozumiane będą jako zorganizowana aktywność państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na

---

[1] *R. Szpyra, Operacje informacyjne państwa w działaniach sił powietrznych. Rozprawa habilitacyjna, Warszawa 2002.*
[2] *R. Stark, Future Warfare: Information Superiority through Info War,* http://www.smsu.edu

zewnętrzne i wewnętrzne systemy informacyjnego komunikowania lub przepływającą przez nie informację.

Operacje informacyjne składają się z trzech głównych komponentów, którymi są: współpraca informacyjna (kooperacja pozytywna); walka informacyjna (kooperacja negatywna) i informacyjne zabezpieczenie. Dwie pierwsze formy aktywności odnoszą się do stosunków między państwami, a więc do relacji zewnętrznych. Tymczasem istnieje jeszcze inny ważny obszar potrzeb. Jest nim zasilanie informacyjne własnych procesów wewnętrznych. Zaspokajanie tych potrzeb jest domeną trzeciej formy: informacyjnego zabezpieczenia.

Walka informacyjna jest formą kooperacji negatywnej operacji informacyjnych. Ponieważ istotą walki jest przemoc, a przedmiotem tej walki są systemy informacyjnego komunikowania przeciwnika oraz przepływająca przez nie informacja, to można przyjąć, że **walka informacyjna to** zorganizowana w formę przemocy aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej przez nie informacji przed podobnym działaniem przeciwnika.

Trzecim komponentem operacji informacyjnych jest informacyjne zabezpieczenie. Jego głównym celem jest zapewnienie właściwego zasilania informacyjnego własnych procesów wewnętrznych. Najważniejszymi z nich są procesy decyzyjne oraz procesy sterowania. Zabezpieczenie to obejmuje zdobywanie informacji, zachodzące w procesach rozpoznania, oraz dostarczanie informacji, realizowane w procesach informacyjnej komunikacji.

Walka informacyjna dzieli się na **informacyjny atak** i **informacyjną obronę**.

Odpowiednio do przyjętego rozumienia walki informacyjnej uznano, iż: ***informacyjny atak*** to zorganizowana w formę przemocy aktywność zewnętrzna prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji.

Informacyjna obrona to zorganizowana aktywność prowadząca do zapewnienia ochrony własnych systemów informacyjnego komunikowania

i przesyłanej przez nie informacji przed rozpoznaniem i informacyjnym atakiem przeciwnika. Warto podkreślić, że obrona ta jest przeciwdziałaniem zarówno przedsięwzięciom rozpoznania, jak i informacyjnego ataku przeciwnika.

W ramach **informacyjnego ataku** mogą być stosowane następujące jego formy:

- **atak informatyczny (w sferze przetwarzania danych cyfrowych);**
- **atak elektroniczny;**
- **atak ogniowy;**
- **działania psychologiczne;**
- **dezinformacja (mylenie).**

Obrona informacyjna obejmuje zapobieganie rozpoznaniu i niedopuszczanie do informacyjnego atakowania lub uzyskiwania pożądanej efektywności tego atakowania przez przeciwnika.

Celem rozpoznania jest uzyskanie informacji o przeciwniku. W aktywności tej wyróżnić można dwa główne elementy: będącą przedmiotem działań informację, która może występować w różnych formach i postaciach, oraz próbujący pozyskać ją element rozpoznania. W tej sytuacji zapobieganie rozpoznaniu może przybierać formę ***przeciwdziałania aktywności rozpoznawczej przeciwnika*** oraz ***ochrony informacji*** przed dostępem elementów rozpoznania.

Przeciwdziałanie aktywności rozpoznawczej przeciwnika polega na odstraszaniu tej aktywności oraz na jej obezwładnianiu, gdy odstraszanie zawiedzie.

Ochrona informacji w rzeczywistości dotyczy zarówno zagrożeń niezwiązanych z działalnością przeciwnika, jak np. wpływ czynników przyrody czy błędy personelu, co może doprowadzić do utraty lub deformacji informacji, jak też zagrożeń wiążących się z działaniami rozpoznawczymi przeciwnika. Przedmiotem niniejszych badań jest przede wszystkim zapobieganie rozpoznaniu przeciwnika, a przez to ochrona przed rozpoznaniem przeciwnika. Ochrona informacji przed rozpoznaniem osiągana jest głównie w wyniku prowadzenia kontrwywiadu, ochrony technicznej, ochrony informatycznej. Ponadto przedsięwzięciami odnoszącymi się do całej sfery ochrony są: bezpieczeństwo działań i maskowanie.

Celem informacyjnego atakowania jest niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji. Podobnie jak w wypadku rozpoznania informacyjne atakowanie można przedstawić w postaci uproszczonego modelu. Model ten składa się z systemów informacyjnego komunikowania i przepływającej przez nie informacji oraz ofensywnych elementów walki informacyjnej przeciwnika i zachodzących między nimi relacji. Zapobieganie informacyjnym atakom może być prowadzone w dwu płaszczyznach: ***przeciwdziałania informacyjnym atakom*** oraz ***ochrony własnej informacji i systemów informacyjnego komunikowania*** przed atakiem.

Całość tych przedsięwzięć ma na celu niedopuszczenie do informacyjnego atakowania własnej informacji i systemów informacyjnego komunikowania przez przeciwnika. Głównym zadaniem w tym względzie jest, zatem ***przeciwdziałanie informacyjnym atakom*** przeciwnika. Przeciwdziałanie to może mieć formę odstraszania tych ataków oraz ich obezwładniania, gdy odstraszanie zawodzi.

Niezależnie od tego prowadzi się przedsięwzięcia, które mają zabezpieczać informację i systemy informacyjnego komunikowania w sytuacji, gdy przeciwdziałanie atakom okaże się nie w pełni skuteczne. Przedsięwzięcia te to ***ochrona własnej informacji i systemów informacyjnego komunikowania***.

Ochronę własnej informacji i systemów informacyjnego komunikowania zapewnia się przez kontrwywiad, ochronę psychologiczną, ochronę elektroniczną, ochronę informatyczną, inżynieryjną rozbudowę i kontrdezinformację. Ponadto przedsięwzięciami odnoszącymi się do całej sfery ochrony są: bezpieczeństwo działań i maskowanie.

Ochrona informacji to przedsięwzięcia podejmowane dla osłony informacji i systemów informacyjnych, zmierzające do zapewnienie ich dostępności, integralności, autentyczności, tajności i zdolności do identyfikowania źródła informacji i danych.

Ochrona informacji obejmuje także odtworzenie systemów informacyjnych przez utrzymywanie zdolności do osłony, wykrywania zagrożeń i reagowania na nie. Ochrona informacji jest stosowana we wszystkich działaniach militarnych na wszystkich szczeblach.

Elementami ochrony własnej informacji i systemów informacyjnego komunikowania są: kontrwywiad, ochrona psychologiczna, ochrona elektroniczna, ochrona informatyczna, inżynieryjna rozbudowa i kontrdezinformacja. Ponadto przedsięwzięciami odnoszącymi się do całej sfery ochrony są: bezpieczeństwo działań i maskowanie.

Założenia te legły u podstaw sformułowania scenariuszy zagrożeń bezpieczeństwa informacyjnego. Zgodnie z nimi zagrożeń bezpieczeństwa informacyjnego upatrywać należy przede wszystkim w informacyjnym ataku oraz w działalności rozpoznawczej. Zagrożenia mogą stanowić efekt celowej działalności ludzkiej oraz oddziaływań środowiska. Scenariusze zagrożeń nie uwzględniają oddziaływań środowiska, gdyż te są dobrze znane i opisane.

Scenariusze koncentrują się na zdarzeniach będących różnymi formami ataku informacyjnego. Charakterystyczne dla poszczególnych form ataku informacyjnego zdarzenia odniesione zostały do trzech podmiotów. Jeden, który reprezentuję skalę mikro a jest nim instytucja rozmieszczona w stosunkowo niewielkim kompleksie reprezentowana przez Akademię Obrony Narodowej. Kolejnym podmiotem jest rozległe miasto – centrum administracyjne, jakim jest Warszawa – stolica państwa. Wreszcie trzecim podmiotem jest państwo średniej wielkości, jakim jest Polska.

Zdanie sobie sprawy z zagrożenia[3], wynikającego z ataku informacyjnego, jest pierwszym krokiem do podjęcia niezbędnych działań, służących zapobieżeniu tej groźbie. Następnym krokiem jest zdefiniowanie potencjalnych celów, które napastnicy mogliby zaatakować w pierwszej kolejności. Już w 1997 roku amerykańscy specjaliści zdefiniowali pojęcie *„infrastruktury krytycznej"* (critical infrastructure), której zniszczenie lub uszkodzenie może osłabić zdolność obronną oraz bezpieczeństwo ekonomiczne państwa.

Określono także **osiem głównych elementów tej infrastruktury**:

- **telekomunikacja (Telecommunication)** — linie telefoniczne, satelity, sieci komputerowe - komercyjne, wojskowe, akademickie itd.;

---

[3] *A. Bógdał-Brzezińska, M.F. Gawrycki, Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Warszawa 2003, s. 134-135.*

- **system energetyczny (Electrical Power System)** - produkcja, przesył i dystrybucja energii, a także transport i magazynowanie surowców niezbędnych do jej produkcji;
- **produkcja, magazynowanie i transport gazu ziemnego i ropy naftowej (Oil and Gas Delivery and Storage)** - cały proces wydobycia ropy naftowej i gazu ziemnego, magazynowania, przetworzenia i transportu za pomocą rurociągów, statków, transportem kołowym i kolejowym (także dostarczanie paliwa do zamorskich baz wojskowych USA);
- **system bankowy i finansowy (Banking and Finance)** - system przepływu bilionów dolarów, poczynając od indywidualnych depozytów po transfer ogromnych sum pieniędzy z jednego krańca świata na drugi. Obejmuje wszystkie dostępne instrumenty operacji finansowych;
- **transport (Transportation)** - transport lotniczy, kolejowy, morski, rzeczny, drogowy osób i towarów oraz cały system wsparcia logistycznego;
- **system zaopatrzenia w wodę (Water Supply System)** - składają się na niego: ujęcia wody, zbiorniki wodne, wodociągi, systemy filtrowania i oczyszczania wody, dostarczania dla rolnictwa, przemysłu, straży pożarnych oraz indywidualnych odbiorców;
- **służby ratownicze (Emergency Service)** - w Stanach Zjednoczonych system alarmowy 911 - komunikacja z policją, służbą zdrowia, strażą pożarną itd.;
- **ciągłość funkcjonowania władzy i służb publicznych (Continuity of Government Serwces)** - wszystkie te elementy, które zapewniają funkcjonowanie lokalnych, regionalnych i centralnych władz oraz systemu publicznego: służba zdrowia, bezpieczeństwo, obrona itd.

Także w Polsce rośnie świadomość potrzeby przygotowania się do potencjalnego cyberataku. We wrześniu 2002 roku w Biurze Bezpieczeństwa Narodowego odbyło się seminarium poświęcone ochronie rodzimej infrastruktury krytycznej (zdefiniowanej podobnie, jak to czynią Amerykanie).

W innym ujęciu[4] krytyczna infrastruktura państwa to:

- obiekty (budynki i budowle) i urządzenia, służby odpowiedzialne za obsługę tych obiektów i urządzeń;
- systemy i sieci teleinformatyczne istotne dla bezpieczeństwa i ekonomicznego dobrobytu państwa oraz jego efektywnego funkcjonowania obejmując:
- systemy energetyczne, telekomunikacyjne, poczty, teleinformatyczne, finansowe i bankowe, zarządzania zasobami wodnymi, dostaw żywności i wody, opieki zdrowotnej, transportu, usługi w zakresie bezpieczeństwa powszechnego i porządku publicznego oraz zapewnienie prawidłowego funkcjonowania najważniejszych struktur administracji publicznej w sytuacjach nadzwyczajnych zagrożeń (w tym centra zarządzania kryzysowego i stanowiska kierowania) oraz ochrony przemysłu o strategicznym znaczeniu, w tym obronnego.

Definicja jest bardzo szeroka, obejmuje wiele - faktycznie - istotnych dziedzin z administracji i gospodarki Polski, które funkcjonując prowadzą wymianę informacji i danych (lokalnie i rozlegle) z wykorzystaniem sieci teleinformatycznych, będących głównym obszarem ataku i infiltracji.

Uogólniając zakres obszarowy, można wyrazić zakres KIP obejmujący:

- telekomunikację;
- systemy energetyczne;
- systemy bankowe i finansowe;
- transport;
- systemy zaopatrywania w wodę;
- system opieki zdrowotnej;
- ratownictwo.

---

[4] *J. Nowak, Elementy bezpieczeństwa teleinformatycznego w sieciach wymiany informacji państwa. Praca studyjna, Warszawa 2003, s. 48-50.*

Należy pamiętać, że obszary te dotyczą zarówno sfery publicznej jak i prywatnej.

Rozpatrując zagadnienia KIP istnieje potrzeba zdefiniowania dwóch pojęć odnoszących się do obiektów potencjalnego oddziaływania zewnętrznego (zasoby) oraz elementów łączące te obiekty (infrastruktura), a mianowicie:

Krytyczne zasoby (aktywa) teleinformatyczne definiowane jako zasoby wykorzystywane dla utrzymania bezpieczeństwa ekonomicznego państwa oraz wykorzystywane w systemie ochrony zdrowia i bezpieczeństwa publicznego,

Krytyczna Infrastruktura teleinformatyczna (KITI) obejmująca systemy i sieci teleinformatyczne niezbędne dla prowadzenia podstawowych działań gospodarczych i funkcjonowania instytucji publicznych państwa.

Jakie w związku z powyższym obszary KITI należałoby rozpatrywać mając na uwadze realizację przedsięwzięć organizacyjno - technicznych bezpieczeństwa TI. Obszary te (tworzące architekturę KITI) są oczywiście ściśle określone i zdefiniowane, ponieważ w codziennej naszej działalności mamy z nimi do czynienia - nie zawsze zdając sobie z tego sprawę tzn.:

- infrastruktura otwarta stanowiąca systemy i sieci teleinformatyczne, do których dostęp możliwy jest przy wykorzystaniu publicznie dostępnych sieci np. serwery informacyjne urzędów administracji publicznej

  (e-administracja), serwery bankowe,

- infrastruktura zamknięta stanowiąca systemy i sieci teleinformatyczne fizyczne lub logiczne (np. przy wykorzystaniu mechanizmów kryptograficznych odseparowane od sieci publicznie dostępnych).

Obie architektury narażone są na ataki bezpośrednie (np. włamania komputerowe (wewnętrzne i zewnętrzne), silne impulsy elektromagnetyczne i ataki pośrednie (np. zakłócenia w zasilaniu spowodowane uszkodzeniami systemów energetycznych).

Przykłady przedmiotów KITI to:

- MSWiA - system zarządzania kryzysowego;
- ministerstwa - dysponenci systemów baz danych;

- Krajowa Izba Rozliczeniowa - systemy rozliczeń międzybankowych;
- podmioty świadczące usługi certyfikacyjne - wykorzystanie podpisu elektronicznego w elektronicznym obiegu informacji;
- służby publiczne - dostęp do baz danych i systemów ewidencji;
- zakłady energetyczne;
- przedsiębiorstwa wodociągów i kanalizacji.

Rozpatrując możliwe ataki - czy to na otwarte czy zamknięte systemy i sieci teleinformatyczne, należy odnieść się do zagadnień ryzyka dla KIT, a z którym to ryzykiem musimy się liczyć realizując zadania związane z ochroną informacji przetwarzanych w tych systemach i sieciach.

Bibliografia

1. Bógdał-Brzezińska, Gawrycki M.F., Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Warszawa 2003, s. 134-135.
2. Nowak J., Elementy bezpieczeństwa teleinformatycznego w sieciach wymiany informacji państwa. Praca studyjna, Warszawa 2003, s. 48-50.
3. Stark R., Future Warfare: Information Superiority through Info War, http://www.smsu.edu
4. Szpyra R., Operacje informacyjne państwa w działaniach sił powietrznych. Rozprawa habilitacyjna, Warszawa 2002.

2.3. SCENARIUSZE ZAGROŻEŃ

Ośrodek lokalny (AON)

Lp.	Rodzaj ataku	Bezpośrednie efekty ataku	Dalsze skutki ataku	Przeciwdziałanie
1	<u>Atak informatyczny</u> Włamanie do sieci przy wykorzystaniu technik „tylnego wejścia" zdalne przejęcie kontroli nad systemem; Przeciążenie serwera, celowe przeciążenie sieci; Atak na pocztę elektroniczną (bomby pocztowe, spam, podrabianie korespondencji); Monitorowanie komunikacji; Złamanie haseł dostępu; Infekcje wirusowe;	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemem - zablokowanie funkcjonowania sieci; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	Kradzież informacji - każda informacja może być celem takiego ataku. Przejęcie numerów kont bankowych, kart kredytowych, danych osobowych, własności intelektualnej; Dokonanie przelewów pieniędzy z konta AON na obce konta; Pobranie z kont pracowników AON pieniędzy; Publiczne udostępnienie numerów kart kredytowych (w Intemecie) - sprawienie kłopotów użytkownikom; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż.	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych. 3. Zorganizowanie ochrony i wdrożenie procedur polityki: <u>Ochrona fizyczna i środowiskowa</u> (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych);

				Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
2	Atak elektroniczny Wyzwolenie impulsów elekromagnetycznych w rejonie węzłów sieci;	Zniszczenie urządzeń elektronicznych i elektrycznych; Zniszczenie centrali telefonicznej.	Paraliż sieci informatycznych; Paraliż sieci telefonicznej;	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

3	Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci łączności.	Zniszczenie centrali telefonicznej i serwerowi;	Zakłócenie pracy sieci informatycznych i łączności. Paraliż pracy sieci informatycznych i łączności;	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
4	Działania psychologiczne Inżynieria społeczna - przekonanie pracownika AON do wprowadzenia złośliwego oprogramowania z wnętrza sieci AON;	Umożliwienie dostępu do sieci informatycznej oraz dostępu do niejawnej informacji;	Zewnętrzny atak informatyczny na sieć; Kradzież niejawnych informacji (np. danych osobowych czy finansowych);	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji;
5	Dezinformacja Rozsyłanie fałszywych informacji kanałami społecznego komunikowania.	Kwestionowanie uczciwych zamiarów komendy uczelni oraz kierownictw jej komórek organizacyjnych; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu uczelni;	Wywoływanie zaniepokojenia, pogarszanie nastrojów, pogarszanie jakości funkcjonowania AON.	Szybka reakcja władz uczelni na fałszywe informacje; Sprawne docieranie do personelu uczelni z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

Ośrodek regionalny (Warszawa)

Lp.	Rodzaj ataku	Bezpośrednie efekty ataku	Dalsze skutki ataku	Przeciwdziałanie
		1. Sieci teleinformatyczne		
1.1.	Atak informatyczny Włamanie do sieci przy wykorzystaniu technik „tylnego wejścia" zdalne przejęcie kontroli nad systemami; Przeciążenia serwerów, celowe przeciążenie sieci; Złamanie haseł dostępu; Atak na pocztę elektroniczną (bomby pocztowe, spam, podrabianie korespondencji); Infekcje wirusowe; Monitorowanie komunikacji.	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami - blokowanie funkcjonowania elementów sieci lub całej sieci; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	Kradzież informacji – np.: przejęcie numerów kont bankowych, kart kredytowych, danych osobowych, własności intelektualnej, informacji biznesowej, zasobów informacyjnych firm i organizacji; Dokonanie przelewów pieniędzy na obce konta; Pobranie z kont użytkowników sieci pieniędzy; Publiczne udostępnienie numerów kart kredytowych (w Intemecie) - sprawienie kłopotów użytkownikom; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Utrata ważnych zasobów informacyjnych.	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych. 3. Zorganizowanie ochrony i wdrożenie procedur polityki: Ochrona fizyczna i środowiskowa (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych);

				Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
1.2.	Atak elektroniczny Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci; Zniszczenie stacji nadawczych telefonii komórkowej.	Paraliż sieci informatycznych; Zakłócenie pracy sieci telefonii komórkowej.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

1.3.	Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central telefonicznych i serwerowi.	Zakłócanie lub paraliżowanie pracy sieci informatycznej i łączności.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
1.4.	Działania psychologiczne Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej oraz dostępu do niejawnej informacji.	Zewnętrzny atak informatyczny na sieć; Kradzież niejawnych informacji (np. danych osobowych czy finansowych).	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.
1.5.	Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz za pośrednictwem innych środków masowej komunikacji.	Kwestionowanie uczciwych zamiarów przywództw i kierownictw organizacji i firm oraz kierownictw ich komórek organizacyjnych; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu.	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania miasta.	Szybka reakcja władz miasta i zarządów firm na fałszywe informacje; Sprawne docieranie do mieszkańców miasta i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.
2. System energetyczny				
2.1.	Atak informatyczny Atak na serwery sterujące pracą sieci energetycznych i przejęcie kontroli	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych;	Paraliż elementów sieci energetycznej miasta lub całej sieci; Kradzież informacji –	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka,

	nad systemami; Przeciążenia serwerów; Złamanie haseł dostępu; Infekcje wirusowe.	Przejęcie kontroli nad systemami - blokowanie funkcjonowania elementów sterowania sieciami energetycznymi; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	osobowej, technicznej finansowej; Publiczne udostępnienie wrażliwej informacji (w Intemecie) - sprawienie kłopotów; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Pojawienie się niepokojów społecznych.	zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: Ochrona fizyczna i środowiskowa (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych) Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystują-

				cymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
2.2.	<u>Atak elektroniczny</u> Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci teleinformatycznej, sterującej pracą sieci energetycznej lub będących elementami sieci energetycznej; Zniszczenie stacji nadawczych łączności radioliniowej.	Zakłócenia w pracy energetycznego systemu łączności. Zakłócenie lub paraliż pracy sieci energetycznej; Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
2.3.	<u>Atak ogniowy</u> Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central sterowania pracą sieci energetycznej i serwerowi.	Zakłócanie lub paraliżowanie pracy sieci informatycznej i łączności systemu energetycznego; Zakłócanie lub paraliżowanie pracy sieci ener-	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

			getycznej; Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	
2.4.	<u>Działania psychologiczne</u> Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej energetyki oraz dostępu do niejawnej informacji.	Zewnętrzny atak informatyczny na sieć; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie sytuacji finansowej oraz poziomu bezpieczeństwa firm energetycznych.	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.
2.5.	<u>Dezinformacja</u> Rozsyłanie fałszywych informacji o przyczynach awarii sieci.	Kwestionowanie uczciwych zamiarów przywództw i kierownictw organizacji i firm oraz kierownictw ich komórek organizacyjnych; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o sytuacji finansowej firm energetycznych.	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania miasta.	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do ludności miasta i personelu organizacji z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

3. System bankowy i finansowy				
3.1.	<u>Atak informatyczny</u> Atak na serwery i przejęcie kontroli nad systemami; Przeciążenia serwerów; Złamanie haseł dostępu; Infekcje wirusowe.	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami - blokowanie funkcjonowania elementów sieci lub całej sieci; Dokonanie przelewów pieniędzy na obce konta; Pobranie z kont użytkowników sieci pieniędzy; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	Blokowanie przelewów finansowych systemu gospodarki; Kradzież informacji - przejęcie numerów kont bankowych, kart kredytowych, danych osobowych, danych struktury i organizacji sieci; Publiczne udostępnienie numerów kart kredytowych (w Intemecie) - sprawienie kłopotów użytkownikom; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Utrata stabilności finansowej firm i instytucji finansowych rozmieszczonych w obrębie miasta. Zawirowania prowadzące do utraty ciągłości finansowych przez banki, brak możliwości wypłat klientom chcącym odzyskać ulokowane w bankach pieniądze;	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: <u>Ochrona fizyczna i środowiskowa</u> (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych) <u>Ochrona informatyczna</u>: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfigu-

			Pojawienie się niepokojów społecznych.	racji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
3.2.	<u>Atak elektroniczny</u> Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci transferów finansowych.	Zakłócenia w pracy instytucji finansowych; Paraliż lokalnych placówek bankowych; Utrata dokumentacji kont klijenckich; Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

3.3.	Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central teleinformatycznych i serwerowni.	Zakłócanie lub paraliż pracy sieci informatycznej i łączności systemu bankowego i finansowego; Utrata dokumentacji kont klijenckich; Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
3.4.	Działania psychologiczne Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemu bankowego i finansowego oraz do niejawnej informacji; Defraudacje finansowe dokonywane przez pracowników banku.	Zewnętrzny atak informatyczny na sieć; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie bezpieczeństwa operacji finansowych oraz straty podmiotów gospodarczych i klientów indywidualnych.	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.
3.5.	Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz miasta i kierownictw organizacji i firm oraz kierownictw ich komórek organizacyjnych;	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania miasta.	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do mieszkańców miasta i personelu organizacji z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

		Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o sytuacji finansowej miasta i firm związanych z miastem.	Próby zachwiania stabilnością finansową i płynnością pracy banków.	
4. System zaopatrywania miasta w wodę, gaz i paliwa				
4.1.	<u>Atak informatyczny</u> Atak na serwery i przejęcie kontroli nad systemami; Przeciążenia serwerów; Złamanie haseł dostępu; Infekcje wirusowe.	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami; Kradzież informacji - przejęcie danych osobowych, danych struktury i organizacji sieci; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na	Blokowanie funkcjonowania elementów sieci lub całej sieci; Dokonanie przelewów pieniędzy na obce konta; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Utrata stabilności finansowej firm i instytucji usługowych rozmieszczonych w obrębie miasta; Zawirowania prowadzące do utraty ciągłości dostaw i usług świadczonych ludności i podmiotom prawnym przez firmy usługowe.	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: <u>Ochrona fizyczna i środowiskowa</u> (kontrola

		dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.		dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych) Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
4.2.	Atak elektroniczny Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci usługowych – zakłócenie pracy	Zakłócenia w pracy instytucji zaopatrywania miasta; Paraliż lokalnych placó-	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawno-

		lub paraliż tych sieci.	wek zaopatrywania; Utrata dokumentacji klijenckich; Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	ści systemu po ataku.
4.3.	<u>Atak ogniowy</u> Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central teleinformatycznych i serwerowni sterujących funkcjonowaniem sieci usługowych (gazowej, wodociągowej, itp.).	Zakłócanie lub paraliż pracy sieci informatycznej i łączności sieci usługowych; Utrata dokumentacji klijenckich; Zakłócanie lub paraliżowanie pracy sieci usługowych. Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
4.4.	<u>Działania psychologiczne</u> Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemu zaopatrywania miasta oraz do niejawnej informacji; Sabotaż wewnętrzny ze strony pozyskanego personelu organizacji usługowych; Defraudacje finansowe	Zewnętrzny atak informatyczny na sieć; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie bezpieczeństwa operacji finansowych oraz straty podmiotów gospodar-	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.

		dokonywane przez pracowników firm zaopatrywania miasta.	czych systemu zaopatrywania miasta i klientów indywidualnych.	
4.5.	Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz miasta i kierownictw organizacji i firm oraz kierownictw ich komórek organizacyjnych; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o sytuacji finansowej miasta i firm związanych z zaopatrywaniem miasta; Rozsiewanie informacji o fatalnym stanie sieci gazowych i zagrożeniach gazowych.	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania miasta. Próby zachwiania stabilnością finansową i płynnością pracy firm zaopatrywania miasta.	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do mieszkańców miasta i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.
5. System transportu ludzi i towarów (drogowy, lotniczy, szynowy, rzeczny)				
5.1.	Atak informatyczny Atak na serwery i przejęcie kontroli nad systemami; Przeciążenia serwerów;	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami - blokowanie	Zakłócenie lub paraliż systemu kontroli ruchu lotniczego i kontroli naziemnej portu lotniczego;	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola

	Złamanie haseł dostępu; Infekcje wirusowe.	funkcjonowania elementów sieci lub całej sieci; Kradzież informacji - przejęcie danych finansowych, osobowych, technicznych, handlowych, itp; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	Zagrożenie katastrofami w ruchu powietrznym kolejowym i drogowym; Dokonanie przelewów pieniędzy na obce konta; Publiczne udostępnienie wrażliwej informacji (w Intemecie) - sprawienie kłopotów użytkownikom; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Utrata wiarygodności przewoźników prowadząca do strat lub bankructw.	nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: Ochrona fizyczna i środowiskowa (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych) Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń infor-

				matycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
5.2.	<u>Atak elektroniczny</u> Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci i urządzeń kontroli funkcjonowania.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci transportowych.	Katastrofy lotnicze, kolejowe i drogowe; Zakłócenie lub paraliż pracy sieci transportowych; Wywołanie strachu i niezadowolenia wśród ludności.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
5.3.	<u>Atak ogniowy</u> Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central teleinformatycznych, serwerowni i urządzeń kontroli ruchu lotniczego, kolejowego i drogowego.	Katastrofy lotnicze, kolejowe i drogowe; Zakłócenie lub paraliż ruchu lotniczego, kolejowego i drogowego – paraliż komunikacyjny miasta; Wywołanie strachu i niezadowolenia wśród ludności.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

5.4.	Działania psychologiczne Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemów transportowych miasta oraz do niejawnej informacji; Sabotaż wewnętrzny ze strony pozyskanego personelu organizacji usługowych; Defraudacje finansowe dokonywane przez pracowników firm transportowych miasta.	Zewnętrzny atak informatyczny na sieć; Zagrożenie bezpieczeństwa ruchu lotniczego, kolejowego i drogowego; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie bezpieczeństwa operacji finansowych oraz straty podmiotów gospodarczych systemów transportowych miasta i klientów indywidualnych.	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.
5.5.	Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz przez inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz miasta i kierownictw organizacji i firm transportowych; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o sytuacji finansowej	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania miasta. Próby zachwiania stabilnością finansową i płynnością pracy firm transportowych miasta.	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do mieszkańców miasta i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

		miasta i firm transportowych miasta; Rozsiewanie dezinformacji o zagrożeniach ruchu lotniczego, kolejowego i drogowego.		
6. System opieki zdrowotnej i świadczeń społecznych				
6.1.	<u>Atak informatyczny</u> Atak na serwery i przejęcie kontroli nad systemami; Przeciążenia serwerów; Złamanie haseł dostępu; Infekcje wirusowe.	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami - blokowanie funkcjonowania elementów sieci lub całej sieci; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	Kradzież informacji - przejęcie informacji medycznej, danych osobowych, finansowych i biznesowych; Dokonanie przelewów pieniędzy na obce konta; Publiczne udostępnienie wrażliwej informacji (w Intemecie) - sprawienie kłopotów użytkownikom; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Pogorszenie bezpieczeństwa finansowego świadczeniobiorców systemu świadczeń społecznych (emerytów, rencistów, bezrobotnych itp.); Utrata stabilności finansowej placówek opieki	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: <u>Ochrona fizyczna i środowiskowa</u> (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych)

			zdrowotnej rozmieszczonych w obrębie miasta. Zawirowania prowadzące do utraty zdolności świadczenia usług medycznych przez szpitale a nawet przychodnie; Wzrost poczucia zagrożenia mieszkańców oraz niezadowolenia społecznego.	Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
6.2.	Atak elektroniczny Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci.	Zniszczenie urządzeń elektronicznych i elektrycznych wykorzystywanych w służbie zdrowia i placówkach świadczeń społecznych.	Utrata informacji klientów systemu świadczeń społecznych, zakłócenia w wypłatach świadczeń; Zakłócenie lub paraliż pracy systemu opieki	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

			zdrowotnej miasta;	
6.3.	Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central teleinformatycznych i serwerowni oraz odcinanie od zasilania.	Utrata informacji klientów systemu świadczeń społecznych, zakłócenia w wypłatach świadczeń; Pogorszenie bezpieczeństwa finansowego świadczeniobiorców systemu świadczeń społecznych (emerytów, rencistów, bezrobotnych itp.); Zakłócenie lub paraliż pracy systemu opieki zdrowotnej miasta; Wywołanie strachu i niezadowolenia wśród ludności.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
6.4.	Działania psychologiczne Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemów opieki zdrowotnej miasta oraz świadczeń społecznych, ujawnienie niejawnej informacji; Sabotaż wewnętrzny ze strony pozyskanego personelu; Defraudacje finansowe	Zewnętrzny atak informatyczny na sieć; Zagrożenie bezpieczeństwa medycznego; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie bezpieczeństwa finansowego świadczeniobiorców sys-	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.

		dokonywane przez pracowników instytucji opieki zdrowotnej i świadczeń społecznych miasta.	temu świadczeń społecznych (emerytów, rencistów, bezrobotnych itp.); Wzrost poczucia zagrożenia i niezadowolenia społecznego.	
6.5.	<u>Dezinformacja</u> Rozsyłanie fałszywych informacji pocztą elektroniczną oraz przez inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz miasta i kierownictw organizacji systemu świadczeń społecznych i placówek opieki zdrowotnej; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o sytuacji finansowej miasta i niemożności wypłaty świadczeń społecznych; Rozpowszechnianie fałszywych informacji o zatrutych lekarstwach i nieznanych mikrobach oraz braku umiejętności personelu medycznego;	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania miasta. Próby zachwiania stabilnością finansową i płynnością pracy systemu świadczeń społecznych i opieki zdrowotnej miasta. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do mieszkańców miasta i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

		Rozsiewanie dezinformacji o nieskuteczności tradycyjnej medycyny.		
7. System zarządzania miastem i dzielnicami				
7.1.	<u>Atak informatyczny</u> Atak na serwery i przejęcie kontroli nad systemami; Przeciążenia serwerów; Złamanie haseł dostępu; Infekcje wirusowe.	Blokowanie połączeń, ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami informatycznymi; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	Blokowanie funkcjonowania elementów sieci lub całej sieci; Kradzież informacji - przejęcie numerów kont bankowych, kart kredytowych, danych osobowych, urzędowych, biznesowych, itp.; Dokonanie przelewów pieniędzy na obce konta; Publiczne udostępnienie wrażliwej informacji (w Intemecie) - sprawienie kłopotów użytkownikom; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Zakłócenie pracy lub paraliż systemu administrowania miastem.	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: <u>Ochrona fizyczna i środowiskowa</u> (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych) <u>Ochrona informatyczna</u>: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym

				dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
7.2.	<u>Atak elektroniczny</u> Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci teleinformatycznych – zakłócenie pracy lub paraliż tych sieci; Zniszczenie stacji nadawczych telefonii komórkowej zakłócenia w pracy sieci.	Utrata informacji administracyjnych; Zakłócenie pracy lub paraliż systemu administrowania miastem. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

7.3.	Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central telefonicznych iserwerowni – paraliż pracy sieci; Zakłócenie pracy lub paraliż systemu administrowania miastem.	Utrata informacji administracyjnych; Zakłócenie pracy lub paraliż systemu administrowania miastem. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
7.4.	Działania psychologiczne Inżynieria społeczna - pozyskiwanie personelu urzędów do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemów administrowania miasta, ujawnienie niejawnej informacji; Sabotaż wewnętrzny ze strony pozyskanego personelu; Defraudacje finansowe dokonywane przez pracowników administracji miasta.	Zewnętrzny atak informatyczny na sieć; Zagrożenie bezpieczeństwa informacyjnego miasta; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie bezpieczeństwa finansowego; Zakłócenia w administrowaniu miastem; Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.

7.5.	Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz przez inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz i kierownictw organizacji systemu administrowania miasta; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o zamiarach władz miasta.	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania miasta. Próby zachwiania stabilnością finansową ipłynnością finansową miasta. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do mieszkańców miasta i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

Państwo (Polska)

Lp.	Rodzaj ataku	Bezpośrednie efekty ataku	Dalsze skutki ataku	Przeciwdziałanie
		1. Sieci teleinformatyczne		
1.1.	Atak informatyczny Włamania do sieci przy wykorzystaniu technik „tylnego wejścia" zdalne przejęcia kontroli nad systemami; Przeciążenia serwerów, celowe przeciążenia sieci; Złamanie haseł dostępu; Atak na pocztę elektroniczną (bomby pocztowe, spam, podrabianie korespondencji); Infekcje wirusowe; Monitorowanie komunikacji.	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami - blokowanie funkcjonowania elementów sieci; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	Kradzież informacji – np.: przejęcie numerów kont bankowych, kart kredytowych, danych osobowych, własności intelektualnej, informacji biznesowej, zasobów informacyjnych firm i organizacji; Dokonanie przelewów pieniędzy na obce konta; Pobranie z kont użytkowników sieci pieniędzy; Publiczne udostępnienie numerów kart kredytowych (w Intemecie) - sprawienie kłopotów użytkownikom; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Utrata ważnych zasobów informacyjnych.	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych. 3. Zorganizowanie ochrony i wdrożenie procedur polityki: Ochrona fizyczna i środowiskowa (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych);

				Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
1.2.	Atak elektroniczny Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci; Uruchomienie urządzeń zakłócających pracę nadajników	Zniszczenie urządzeń elektronicznych i elektrycznych sieci; Zniszczenie stacji nadawczych telefonii komórkowej; Zakłócenie pracy stacji	Paraliż sieci informatycznych; Zakłócenie pracy sieci telefonii komórkowej.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Uodpornienie urządzeń na zakłócanie; Zorganizowanie systemu wykrywania i neutralizacji nadajników zakłócających; Zorganizowanie systemu odtwarzania sprawno-

	łączności bezprzewodowej.	nadawczych telefonii komórkowej.		ści systemu po ataku.
1.3.	Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central telefonicznych i serwerowi.	Zakłócanie lub paraliżowanie pracy sieci informatycznej i łączności.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
1.4.	Działania psychologiczne Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej oraz dostępu do niejawnej informacji.	Zewnętrzny atak informatyczny na sieć; Kradzież niejawnych informacji (np. danych osobowych czy finansowych).	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.
1.5.	Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz za pośrednictwem innych środków masowej komunikacji.	Kwestionowanie uczciwych zamiarów przywództw i kierownictw organizacji i firm oraz kierownictw ich komórek organizacyjnych; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu.	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania państwa.	Szybka reakcja władz państwa i zarządów firm na fałszywe informacje; Sprawne docieranie do ludności i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.
2. System energetyczny				
2.1.	Atak informatyczny Atak na serwery sterujące pracą sieci	Blokowanie połączeń - ograniczenie przepu-	Paraliż elementów sieci energetycznej państwa	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym:

	energetycznych i przejęcie kontroli nad systemami; Przeciążenia serwerów; Złamanie haseł dostępu; Infekcje wirusowe.	stowości łączy sieciowych; Przejęcie kontroli nad systemami - blokowanie funkcjonowania elementów sterowania sieciami energetycznymi; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	lub całej sieci; Kradzież informacji – osobowej, technicznej finansowej; Publiczne udostępnienie wrażliwej informacji (w Intemecie) - sprawienie kłopotów; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Pojawienie się niepokojów społecznych.	1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: Ochrona fizyczna i środowiskowa (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych) Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed

				atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
2.2.	<u>Atak elektroniczny</u> Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci; Uruchomienie urządzeń zakłócających pracę nadajników łączności bezprzewodowej.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci teleinformatycznej, sterującej pracą sieci energetycznej lub będących elementami sieci energetycznej; Zniszczenie stacji nadawczych łączności radioliniowej; Zakłócenie pracy radioliniowych stacji nadawczych.	Zakłócenia w pracy energetycznego systemu łączności. Zakłócenie lub paraliż pracy sieci energetycznej; Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
2.3.	<u>Atak ogniowy</u> Zdetonowanie ładunków wybucho-	Zniszczenie central sterowania pracą sieci energetycznej i serwe-	Zakłócanie lub paraliżowanie pracy sieci informatycznej i łączności systemu	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawno-

	wych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	rowi.	systemu energetycznego; Zakłócanie lub paraliżowanie pracy sieci energetycznej; Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	ści systemu po ataku.
2.4.	<u>Działania psychologiczne</u> Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej energetyki oraz dostępu do niejawnej informacji.	Zewnętrzny atak informatyczny na sieć; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie sytuacji finansowej oraz poziomu bezpieczeństwa firm energetycznych.	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.
2.5.	<u>Dezinformacja</u> Rozsyłanie fałszywych informacji o przyczynach awarii sieci.	Kwestionowanie uczciwych zamiarów przywództw i kierownictw organizacji i firm oraz kierownictw ich komórek organizacyjnych; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o sy-	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania państwa.	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do ludności i personelu organizacji z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

		o sytuacji finansowej firm energetycznych.		
3. System bankowy i finansowy				
3.1.	<u>Atak informatyczny</u> Atak na serwery i przejęcie kontroli nad systemami; Przeciążenia serwerów; Złamanie haseł dostępu; Infekcje wirusowe.	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami - blokowanie funkcjonowania elementów sieci; Dokonanie przelewów pieniędzy na obce konta; Pobranie z kont użytkowników sieci pieniędzy; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych	Blokowanie przelewów finansowych systemu gospodarki; Kradzież informacji - przejęcie numerów kont bankowych, kart kredytowych, danych osobowych, danych struktury i organizacji sieci; Publiczne udostępnienie numerów kart kredytowych (w Intemecie) - sprawienie kłopotów użytkownikom; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Utrata stabilności finansowej firm i instytucji finansowych rozmieszczonych w obrębie państwa. Zawirowania prowadzące do utraty ciągłości finansowych przez banki, brak możliwości wypłat klientom chcącym odzyskać ulokowane w bankach pieniądze;	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: <u>Ochrona fizyczna i środowiskowa</u> (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych) <u>Ochrona informatyczna</u>: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed pró-

		podzespołów stacji roboczych i serwerów.	Pojawienie się niepokojów społecznych.	bami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
3.2.	<u>Atak elektroniczny</u> Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci transferów finansowych.	Zakłócenia w pracy instytucji finansowych; Paraliż lokalnych placówek bankowych; Utrata dokumentacji kont klijenckich; Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

3.3.	Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central teleinformatycznych i serwerowni.	Zakłócanie lub paraliż pracy sieci informatycznej i łączności systemu bankowego i finansowego; Utrata dokumentacji kont klijenckich; Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
3.4.	Działania psychologiczne Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemu bankowego i finansowego oraz do niejawnej informacji; Defraudacje finansowe dokonywane przez pracowników banków.	Zewnętrzny atak informatyczny na sieć; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie bezpieczeństwa operacji finansowych oraz straty podmiotów gospodarczych i klientów indywidualnych.	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.
3.5.	Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz miasta i kierownictw organizacji i firm oraz kierownictw ich komórek organizacyjnych; Podważanie wiarygod-	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania państwa. Próby zachwiania stabilnością finansową	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do mieszkańców miasta i personelu organizacji z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

		ności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o sytuacji finansowej państwa i firm w jego obszarze.	nością finansową i płynnością pracy banków.	
4. Systemy zaopatrywania w wodę, gaz i paliwa				
4.1.	<u>Atak informatyczny</u> Atak na serwery i przejęcie kontroli nad systemami; Przeciążenia serwerów; Złamanie haseł dostępu; Infekcje wirusowe.	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami; Kradzież informacji - przejęcie danych osobowych, danych struktury i organizacji sieci; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków kom-	Blokowanie funkcjonowania elementów sieci lub całej sieci; Dokonanie przelewów pieniędzy na obce konta; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Utrata stabilności finansowej firm i instytucji usługowych; Zawirowania prowadzące do utraty ciągłości dostaw i usług świadczonych ludności i podmiotom prawnym przez firmy usługowe.	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: <u>Ochrona fizyczna i środowiskowa</u> (kontrola dostępu; ochrona przed pożarami, awariami

		puterowych i innych podzespołów stacji roboczych i serwerów.		systemów zasilania i obsługi; ochrona przed przechwyceniem danych) Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
4.2.	Atak elektroniczny Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci usługowych – zakłócenie pracy lub paraliż tych sieci.	Zakłócenia w pracy instytucji zaopatrywania miasta; Paraliż lokalnych placówek zaopatrywania;	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

			Utrata dokumentacji klijenckich; Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	
4.3.	Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central teleinformatycznych i serwerowni sterujących funkcjonowaniem sieci usługowych (gazowej, wodociągowej, itp.).	Zakłócanie lub paraliż pracy sieci informatycznej i łączności sieci usługowych; Utrata dokumentacji klijenckich; Zakłócanie lub paraliżowanie pracy sieci usługowych. Wzrost niezadowolenia społecznego i pojawienie się niepokojów.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
4.4.	Działania psychologiczne Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemu zaopatrywania miasta oraz do niejawnej informacji; Sabotaż wewnętrzny ze strony pozyskanego personelu organizacji usługowych; Defraudacje finansowe dokonywane przez pracowników firm zaopa-	Zewnętrzny atak informatyczny na sieć; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie bezpieczeństwa operacji finansowych oraz straty podmiotów gospodarczych systemu zaopatrywania instytucji	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.

		trywania instytucji i ludności.	i klientów indywidualnych.	
4.5.	Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz miasta i kierownictw organizacji i firm oraz kierownictw ich komórek organizacyjnych; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o sytuacji finansowej państwa i firm związanych z zaopatrywaniem; Rozsiewanie informacji o fatalnym stanie sieci gazowych i zagrożeniach gazowych.	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania miasta. Próby zachwiania stabilnością finansową i płynnością pracy firm zaopatrywania.	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do ludności i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.
5. System transportu ludzi i towarów (drogowy, lotniczy, szynowy, rzeczny)				
5.1.	Atak informatyczny Atak na serwery i przejęcie kontroli nad systemami; Przeciążenia serwerów; Złamanie haseł dostępu;	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami - blokowanie funkcjonowania elementów sieci lub całej sieci;	Zakłócenie lub paraliż systemu kontroli ruchu lotniczego i kontroli naziemnej portu lotniczego; Zagrożenie katastrofami w ruchu powietrznym	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola

	Infekcje wirusowe.	Kradzież informacji - przejęcie danych finansowych, osobowych, technicznych, handlowych, itp; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	kolejowym i drogowym; Dokonanie przelewów pieniędzy na obce konta; Publiczne udostępnienie wrażliwej informacji (w Intemecie) - sprawienie kłopotów użytkownikom; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Utrata wiarygodności przewoźników prowadząca do strat lub bankructw.	sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: Ochrona fizyczna i środowiskowa (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych) Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona

				przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
5.2.	Atak elektroniczny Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci i urządzeń kontroli funkcjonowania.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci transportowych.	Katastrofy lotnicze, kolejowe i drogowe; Zakłócenie lub paraliż pracy sieci transportowych; Wywołanie strachu i niezadowolenia wśród ludności.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
5.3.	Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central teleinformatycznych, serwerowni i urządzeń kontroli ruchu lotniczego, kolejowego i drogowego.	Katastrofy lotnicze, kolejowe i drogowe; Zakłócenie lub paraliż ruchu lotniczego, kolejowego i drogowego – paraliż komunikacyjny; Wywołanie strachu i niezadowolenia wśród ludności.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

5.4.	<u>Działania psychologiczne</u> Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemów transportowych miasta oraz do niejawnej informacji; Sabotaż wewnętrzny ze strony pozyskanego personelu organizacji usługowych; Defraudacje finansowe dokonywane przez pracowników firm transportowych.	Zewnętrzny atak informatyczny na sieć; Zagrożenie bezpieczeństwa ruchu lotniczego, kolejowego i drogowego; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie bezpieczeństwa operacji finansowych oraz straty podmiotów gospodarczych systemów transportowych i klientów indywidualnych.	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.
5.5.	<u>Dezinformacja</u> Rozsyłanie fałszywych informacji pocztą elektroniczną oraz przez inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz miasta i kierownictw organizacji i firm transportowych; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o sytuacji finansowej firm transportowych;	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania miasta. Próby zachwiania stabilnością finansową i płynnością pracy firm transportowych.	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do ludności i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

		Rozsiewanie dezinformacji o zagrożeniach ruchu lotniczego, kolejowego i drogowego.		
6. System opieki zdrowotnej i świadczeń społecznych				
6.1.	<u>Atak informatyczny</u> Atak na serwery i przejęcie kontroli nad systemami; Przeciążenia serwerów; Złamanie haseł dostępu; Infekcje wirusowe.	Blokowanie połączeń - ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami - blokowanie funkcjonowania elementów sieci lub całej sieci; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	Kradzież informacji - przejęcie informacji medycznej, danych osobowych, finansowych i biznesowych; Dokonanie przelewów pieniędzy na obce konta; Publiczne udostępnienie wrażliwej informacji (w Intemecie) - sprawienie kłopotów użytkownikom; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Pogorszenie bezpieczeństwa finansowego świadczeniobiorców systemu świadczeń społecznych (emerytów, rencistów, bezrobotnych itp.); Utrata stabilności finansowej placówek opieki zdrowotnej; Zawirowania prowadzą-	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: <u>Ochrona fizyczna i środowiskowa</u> (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych) <u>Ochrona informatyczna</u>: filtry i zapory sieciowe (ochrona wewnętrznej sieci informa-

			ce do utraty zdolności świadczenia usług medycznych przez szpitale a nawet przychodnie; Wzrost poczucia zagrożenia mieszkańców oraz niezadowolenia społecznego.	tycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
6.2.	<u>Atak elektroniczny</u> Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci.	Zniszczenie urządzeń elektronicznych i elektrycznych wykorzystywanych w służbie zdrowia i placówkach świadczeń społecznych.	Utrata informacji klientów systemu świadczeń społecznych, zakłócenia w wypłatach świadczeń; Zakłócenie lub paraliż pracy systemu opieki zdrowotnej;	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

6.3.	Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central teleinformatycznych i serwerowni oraz odcinanie od zasilania.	Utrata informacji klientów systemu świadczeń społecznych, zakłócenia w wypłatach świadczeń; Pogorszenie bezpieczeństwa finansowego świadczeniobiorców systemu świadczeń społecznych (emerytów, rencistów, bezrobotnych itp.); Zakłócenie lub paraliż pracy systemu opieki zdrowotnej; Wywołanie strachu i niezadowolenia wśród ludności.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
6.4.	Działania psychologiczne Inżynieria społeczna - pozyskiwanie personelu organizacji do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemów opieki zdrowotnej miasta oraz świadczeń społecznych, ujawnienie niejawnej informacji; Sabotaż wewnętrzny ze strony pozyskanego personelu; Defraudacje finansowe dokonywane przez pra-	Zewnętrzny atak informatyczny na sieć; Zagrożenie bezpieczeństwa medycznego; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie bezpieczeństwa finansowego świadczeniobiorców systemu świadczeń społecznych (emerytów,	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.

		cowników instytucji opieki zdrowotnej i świadczeń społecznych.	rencistów, bezrobotnych itp.); Wzrost poczucia zagrożenia i niezadowolenia społecznego.	
6.5.	<u>Dezinformacja</u> Rozsyłanie fałszywych informacji pocztą elektroniczną oraz przez inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz miasta i kierownictw organizacji systemu świadczeń społecznych i placówek opieki zdrowotnej; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o sytuacji finansowej państwa i niemożności wypłaty świadczeń społecznych; Rozpowszechnianie fałszywych informacji o zatrutych lekarstwach i nieznanych mikrobach oraz braku umiejętności personelu medycznego; Rozsiewanie dezinformacji o nieskuteczności tradycyjnej medycyny.	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania państwa. Próby zachwiania stabilnością finansową i płynnością pracy systemu świadczeń społecznych i opieki zdrowotnej; Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do ludności i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

7. System zarządzania państwem				
7.1.	Atak informatyczny Atak na serwery i przejęcie kontroli nad systemami; Przeciążenia serwerów; Złamanie haseł dostępu; Infekcje wirusowe.	Blokowanie połączeń, ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemami informatycznymi; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.	Blokowanie funkcjonowania elementów sieci lub całej sieci; Kradzież informacji - przejęcie numerów kont bankowych, kart kredytowych, danych osobowych, urzędowych, biznesowych, itp.; Dokonanie przelewów pieniędzy na obce konta; Publiczne udostępnienie wrażliwej informacji (w Intemecie) - sprawienie kłopotów użytkownikom; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Zakłócenie pracy lub paraliż systemu administrowania państwem.	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: 1. Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). 2. Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych 3. Zorganizowanie ochrony i wdrożenie procedur polityki: Ochrona fizyczna i środowiskowa (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych) Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfigu-

				racji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. 4. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
7.2.	<u>Atak elektroniczny</u> Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci; Uruchomienie urządzeń zakłócających pracę nadajników łączności bezprzewodowej.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci teleinformatycznych – zakłócenie pracy lub paraliż tych sieci; Zniszczenie stacji nadawczych telefonii komórkowej zakłócenia w pracy sieci; Zakłócenie pracy stacji nadawczych telefonii bezprzewodowej.	Utrata informacji administracyjnych; Zakłócenie pracy lub paraliż systemu administrowania miastem. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.

7.3.	Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central telefonicznych i serwerowni – paraliż pracy sieci; Zakłócenie pracy lub paraliż systemu administrowania miastem.	Utrata informacji administracyjnych; Zakłócenie pracy systemu administrowania państwem. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
7.4.	Działania psychologiczne Inżynieria społeczna - pozyskiwanie personelu urzędów do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemów administrowania państwem, ujawnienie niejawnej informacji; Sabotaż wewnętrzny ze strony pozyskanego personelu; Defraudacje finansowe dokonywane przez pracowników administracji.	Zewnętrzny atak informatyczny na sieć; Zagrożenie bezpieczeństwa informacyjnego państwa; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie bezpieczeństwa finansowego; Zakłócenia w administrowaniu państwem; Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.
7.5.	Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz przez inne	Kwestionowanie uczciwych zamiarów władz i kierownictw organizacji systemu administrowa-	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogar-	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do ludności i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu;

	środki komunikowania społecznego.	nia państwem; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o zamiarach władz państwa; Podawanie fałszywych informacji o pracy na rzecz interesów obcych państw i organizacji przez przedstawicieli władz.	szanie jakości funkcjonowania państwa. Próby zachwiania stabilnością finansową i płynnością finansową państwa. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i napiętnowanie dezinformatorów.

2.4. ZAŁOŻENIA DLA SYMULACYJNEGO BADANIA WALKI INFORMACYJNEJ (MODEL INFOWARFARE) I ANALIZY JEJ WPŁYWU NA BEZPIECZEŃSTWO ORGANIZACJI (PAŃSTWA). PRZEPROWADZENIE EKSPERYMENTÓW SYMULACYJNYCH

„W ciągu ostatnich kilku lat dramatycznie wzrosły zagrożenia w cyberprzestrzeni. Polityką Stanów Zjednoczonych jest ochrona przeciwko zniszczeniom systemów informacyjnych krytycznej infrastruktury państwa jak również pomoc w ochronie ludzi, gospodarki i bezpieczeństwa narodowego państwa. Musimy działać w kierunku zmniejszania podatności na te zagrożenia nim one wystąpią i upewnienia się, że zniszczenia w cyberprzestrzeni są bardzo rzadkie, krótkotrwałe, sterowalne (dające sobą zarządzać) i generują minimalne straty."[1]

2.4.1. Prawne aspekty wojny informacyjnej

Rozwój technologiczny przenoszący działalność człowieka w coraz nowe obszary oraz dający mu dostęp do niedostępnych dotychczas obszarów powoduje, że obowiązujące prawo musi znaleźć nowe definicje określające te działania. Tak jak odpowiedzią na zdobycie Kosmosu, czy lądowanie na Księżycu były podpisane pod auspicjami Organizacji Narodów Zjednoczonych porozumienia regulujące ich eksplorację, tak również wykreowanie kolejnego obszaru aktywności jakim jest cyberprzestrzeń wymusza zrewidowanie i zaktualizowanie wielu obowiązujących pojęć.

Jednym z takich pojęć opisujących wzajemne relacje między państwami jest wojna definiowana jako zjawisko społeczno - polityczne polegające na podjęciu decyzji o walce zbrojnej przez podmioty prawa międzynarodowego. Wojna na ogół wiąże się z momentem zerwania stosunków pokojowych i przejścia do stosunków wojennych. Jest kontynuacją polityki państwa prowadzonej innymi środkami. Użycie siły nie jest zawsze tożsame z wojną zaś w czasie rzeczywistej wojny mogą być utrzymywane stosunki dyplomatyczne. Ze względu na rodzaj działań wojennych rozróżnia się wojny konwencjonalne, jądrowe, partyzanckie i inne, natomiast zasięg decyduje

---

[1] *George W. Bush: We wstępie do „The National Strategy to Secure Cyberspace", luty 2003*

o tym czy mówimy o wojnie lokalnej czy światowej.[2] Pod pojęciem siły w stosunkach międzynarodowych rozumie się zespół czynników decydujących o zdolności państw do skutecznego funkcjonowania i obrony własnych interesów w stosunkach międzynarodowych. Potęga państwa zależy w znacznej mierze od jego sił zbrojnych i zdolności do ich użycia aczkolwiek dostrzegalne jest malejące znaczenie siły militarnej na rzecz innych aspektów pozwalających na uzyskanie przewagi.

Państwa mogą z równą skutecznością posługiwać się siłą ekonomiczną, cywilizacyjną jak i kulturalną, i to te czynniki coraz częściej decydują o tym, że państwo staje się mocarstwem. Samo posiadanie siły militarnej nie gwarantuje rzeczywistego bezpieczeństwa państwa, jego potęgi, tak jak brak liczącej się siły militarnej nie musi przeszkadzać w rozbudowywaniu wpływu na stosunki międzynarodowe. Te pozamilitarne przejawy siły mogą lepiej służyć stabilizacji w świecie, ale też możliwe jest stosowanie ich w celach agresywnych. Zdecydowanie trudniej jest w takich sytuacjach zbudować system norm prawnych postępowania i przeciwstawić się dominacji. Jeszcze trudniej określić reguły postępowania wobec najnowszego zjawiska – siły związanej z rewolucją informacyjną. Osobną, bardzo aktualną i kontrowersyjną kwestią jest przyzwolenie prawne i polityczne na użycie siły, w tym przede wszystkim militarnej w stosunkach międzynarodowych do rozwiązywania czy wygaszania konfliktów. „Wymuszanie" pokoju może służyć dobru całej społeczności międzynarodowej, chociaż bez względu na szlachetne motywy takie metody naruszają normy pokojowego rozwiązywania sporów, zasadę suwerenności państw, rodzą zagrożenie nadużycia uprawnień i potrzebę nowego systemu międzynarodowej kontroli użycia siły w ramach ONZ lub regionalnych struktur bezpieczeństwa, jak np. KBWE/OBWE, NATO, OPA, OJA.

Tradycyjnie wojna kojarzona jest z siłami zbrojnymi i przemocą. Artykuł 2 punkt 4 Karty Narodów Zjednoczonych[3] zabrania grożenia użyciem lub użycia siły przeciwko integralności czy niezależności innych państw. Agresja jest określona jako użycie sił zbrojnych przeciwko suwerenności, integralności terytorialnej lub politycznej niezależności innego państwa jednocześnie nie jest agresją odpowiedź państwa

---

[2] *Wielka Internetowa Encyklopedia Multimedialna*

[3] *Wszyscy członkowie powstrzymają się w swych stosunkach międzynarodowych od groźby użycia siły lub użycia jej przeciwko integralności terytorialnej lub niezawisłości politycznej któregokolwiek państwa bądź w jakikolwiek inny sposób niezgodny z celami Organizacji Narodów Zjednoczonych. „Karta Narodów Zjednoczonych", 26.06.1945, San Francisco*

na zbrojny atak[4]. Tak sformułowana definicja pozwala na ujęcie wśród aktów agresji między innymi takich działań jak:

- inwazja lub atak wykonany przez siły zbrojne jednego państwa na terytorium innego, zbrojna okupacja, nawet czasowa, będąca efektem tego ataku, lub jakakolwiek aneksja całości lub części terytorium innego kraju zrealizowana z użyciem siły;
- bombardowanie, lub użycie innej broni przeciwko terytorium innego państwa;
- blokada portów i / lub wybrzeży państwa przez siły zbrojne innego państwa;
- zezwolenie innemu państwu na przygotowanie i przeprowadzenie agresji z własnego terytorium przeciwko trzeciemu państwu;
- wysyłanie lub przepuszczanie przez własne terytorium grup zbrojnych dokonujących aktów zbrojnych na terenie innego państwa;
- inne.

Można ogólnie powiedzieć, że określenie agresja w prawodawstwie międzynarodowym ma związek z użyciem sił zbrojnych i w większości spornych sytuacji międzynarodowych tak jest interpretowane. W 1977 r. Protokół Dodatkowy do Konwencji Genewskiej zdefiniował atak jako „akt przemocy, zarówno ofensywny jak i defensywny, przeciwko adwersarzowi".

Wszystkie te rozważania mają stosunkowo łatwą interpretację przy działaniach bojowych prowadzonych w czterech dotychczas rozpoznanych i wykorzystywanych wymiarach: na ziemi, lądzie, w morzu i przestrzeni kosmicznej. Istnieje szereg aktów prawnych pozwalających na rozwinięcie przywołanych tu definicji w celu określenia strony agresora czy stanu wojny. Znacznie trudniej jest określić w ten sam sposób działania realizowane w trakcie tzw. wojny informacyjnej, ale i tutaj istnieje kilka form ataku, które można uznać za agresję[5], np. uderzenie precyzyjnymi środkami rażenia w wojskowe środki łączności, czy zbombardowanie centrów dowodzenia. Istnieje natomiast wiele, które na pewno należą do działań agresywnych ale w sensie prawa międzynarodowego za takie uznane być nie mogą, np. zaatakowanie przez hakerów, bądź wirusami systemów informatycznych pomocy społecznej. Ataki takie przepro-

---

[4] *artykuł 51 Karty Narodów Zjednoczonych*

[5] *Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo: Information Warfare and International Law, National Defense University Press,*

wadzane w ramach działań wojny informacyjnej porównać można do morskiej blokady portów; obydwie te formy działań nie są wprost śmiertelne dla obywateli państwa zaatakowanego jednakże przynoszą podobne, bardzo poważne skutki takie jak sparaliżowanie transportu ludzi i towarów, destrukcję gospodarki czy blokadę informacyjną. Oczywiście obie te formy działań należy rozpatrywać w kontekście konkretnej epoki historycznej a zwłaszcza technologicznej. Podstawową różnicą w ich realizacji jest użycie do blokady portów sił marynarki wojennej (a więc sił zbrojnych) podczas gdy blokada systemów informacyjnych realizowana w najróżniejszy sposób może być wykonywana bez zaangażowania sił wojska. Omówione powyżej implikacje mają decydujące znaczenie dla określenia czy konkretne działania podejmowane w cyberprzestrzeni możemy zgodnie z prawem międzynarodowym uznać za akty: wojny, użycia siły czy też agresji czy nie, a także czy podjęte przeciwdziałania są proporcjonalne do zaistniałych okoliczności. Rozważając tę problematykę należy sobie odpowiedzieć na pytanie: czy zaistniałe zdarzenie, które społeczeństwo, państwo, odczuwa jako atak na jego suwerenność jest rzeczywiście agresją. Staje się to szczególnie ważne gdy w otoczeniu międzynarodowym nie daje się zauważyć oznak narastającego konfliktu. Może się zdarzyć, że wystąpienie przypadkowego zjawiska np. wynikającego z istniejących w oprogramowaniu problemów (błędów, konfliktów) potraktowane zostanie jako cyberatak. Trudny do zidentyfikowania jest również prawdziwy sprawca ataku. Jednymi z najbardziej spektakularnych przykładów potraktowania przypadkowych błędów oprogramowania jako ataków cyberterrorystów było unieruchomienie sieci telekomunikacyjnej dalekiego zasięgu firmy AT&T na przeciąg dziewięciu godzin w 1990 roku, zbombardowanie angielskiego lotniskowca przez własnego pilota w 1992r. czy dwie katastrofy amerykańskich myśliwców F-117. Błędy te mogą mieć różne przyczyny ale jedną z najpoważniejszych jest nieuwaga i niedbałość twórców oprogramowania jak np. przypadek, który zdarzył się twórcom bardzo popularnego programu Photoshop, którzy w ostatecznej wersji programu pozostawili „bombę czasową" unieruchomiającą program po przekroczeniu pewnej daty, co było pozostałością po wersji testowej programu.[6]

Wyjaśnianie nieporozumień między państwami na drodze negocjacji jest podstawową drogą przewidzianą do ich rozstrzygania i chociaż cytowany 51 artykuł Karty Narodów Zjednoczonych daje możliwość odpowiedzi na atak z użyciem siły to

---

[6] *Lawrence T. Greenberg i in.: op.cit.*

jest to sprawa niezwykle kontrowersyjna, zwłaszcza jeżeli chodzi o skalę tej odpowiedzi. Jak powiedziano wcześniej akt agresji realizowany w cyberprzestrzeni ma niewiele wspólnego z sankcjonowaną przez prawo możliwością kontruderzenia. Oznacza to, że prawo międzynarodowe w jego obecnej postaci nie pozwala na odpowiedź państwa będącego obiektem działań wojennych w przestrzeni wirtualnej na odpowiedź środkami przewidzianymi do odparcia agresji militarnej. Dyskusje nad sposobem zakwalifikowania ataku na sieć komputerową jako aktu agresji czy wojny będzie z pewnością jeszcze długo trwała a jej podstawę musi stanowić ocena skutków wywołanych przez ten atak. Jeżeli zaatakowana zostanie sieć lotniczej firmy transportowej w celu wykradzenia danych o strategii firmy czy jej klientach to będziemy mieli do czynienia z kradzieżą, którą należy traktować jako przestępstwo z użyciem komputera, jeżeli natomiast w wyniku tego ataku nastąpi wypadek, czy kolizja samolotów to mamy już wówczas do czynienia z aktem agresji, który z pewnością zgodnie z normami międzynarodowymi można uznać za zbrojny atak, mimo że nie użyto żadnych środków dotychczas uznawanych za środki przemocy zbrojnej.

Z całkowitą pewnością można powiedzieć, że współczesne prawo międzynarodowe nie jest przygotowane do rozstrzygania problemów występujących między międzynarodowymi uregulowaniami dotyczącymi suwerenności państw a możliwościami sieci globalnej. Stwarza to pole do prowadzenia działań wrogich bez jakichkolwiek konsekwencji na arenie międzynarodowej lub z konsekwencjami niewspółmiernymi do wyrządzonych szkód. Szczególnie duże możliwości stają przed państwami przodującymi w rozwoju technologii informatycznych. Stany Zjednoczone, wykorzystując swoją dominującą rolę w świecie, zarówno w tej jak i wielu innych dziedzinach, dążą do nakreślenia granic między przestępczością komputerową a wojną informacyjną. Uznanie za akty wojny czy użycia sił również ataków nie wywołujących skutków śmiertelnych będzie miało daleko idące konsekwencje w rozstrzyganiu sporów międzynarodowych. Zrealizowanie koncepcji zrównującej wszystkie ataki na zasoby informacyjne jako akty agresji w podobny sposób jak montrealska konwencja, uznająca wszystkie akty przeciwko lotnictwu cywilnemu za akty wrogie, da możliwość skutecznej prawnej ochrony zarówno wojskowych jak i cywilnych systemów informacyjnych przed atakami hakerskimi.

Nasycenie w miarę otwartymi[7] systemami informatycznymi różnych gałęzi życia zapewniających spokojną realizację pokojowych celów państw i narodów powoduje, że ich ochrona staje się sprawą priorytetową. Definicja Krytycznej Infrastruktury Państwa jako podstawowego zasobu informacyjnego decydującego o sprawnym działaniu tego organizmu społecznego narzuca konieczność jego ochrony w sposób adekwatny do zagrożeń a co za tym idzie również do egzekwowania prawa do odpowiedzi na akty agresji przeciwko nim. Skoro mamy do czynienia z możliwością uznania każdego aktu skierowanego przeciwko sieci jako aktu agresji to pozostaje do rozwiązania kwestia ewentualnej kontroli nad rozwojem środków służących tego typu aktom, swego rodzaju Układ o Nie-rozprzestrzenianiu Broni Informacyjnej, ale w chwili obecnej wydaje się to niewykonalne. O ile wszystkie środki poddawane kontroli zbrojeń w dotychczasowych uregulowaniach prawnych były z założenia przeznaczone do celów militarnych to rozwiązania (technologie), które mogą być użyte jako narzędzia ataku informacyjnego mają głównie cywilne przeznaczenie. Staje się potrzebą chwili dążenie do uregulowania problematyki bezpieczeństwa informacji na płaszczyźnie międzynarodowej i wprowadzenie takich rozwiązań, które będą obligowały państwa do ścigania przestępstw komputerowych na równi z innymi zagrożeniami terrorystycznymi.

2.4.2. Bezpieczeństwo informacyjne jako element bezpieczeństwa narodowego

Wszystkie dotychczasowe doświadczenia wskazują, że rozwój technologii informacyjnych prowadząc do rozwoju społeczeństw może również doprowadzić do konfliktu, który z pewnością można będzie nazwać wojną informacyjną. Wojna ta będzie wojną globalną, jako że globalny jest zasięg sieci teleinformatycznych. Szczególne znaczenie w tego rodzaju działaniach będzie mieć pierwsze uderzenie.[8] Istnieje duży związek pomiędzy zakresem zniszczeń jakich doznał nieprzyjacielski system informacyjny a jego możliwością odpowiedzi z wykorzystaniem środków prowadzenia działań wojny informacyjnej ale również klasycznej. Prowadzenie działań wojny informacyjnej jest stosunkowo niedrogie w porównaniu z działaniami i uzbrojeniem tradycyjnym. Jeżeli chcesz zniszczyć serce gospodarki przemysłowej musisz zniszczyć

---

[7] *dostępnymi dla użytkowników sieci globalnej*

[8] *Mathew G. Devost: Political Aspects of Class III Information Warfare: Global Conflict and Terrorism, InfoWarCon II, Montreal 1995*

fizycznie fabryki, natomiast do zniszczenia gospodarki informacyjnej wystarczy zniszczyć lub ograniczyć przepływ informacji co jest o wiele mniej kosztowne niż pierwsza z tych opcji. W naukach politycznych mamy do czynienia z dwoma podejściami do bezpieczeństwa narodowego; liberalne i realistyczne. Drugie z nich koncentruje się na bezpieczeństwie w jego militarnym wymiarze, a więc posiadaniu odpowiednio silnego potencjału militarnego, który pozwoli na zachowanie pożądanego poziomu bezpieczeństwa państwa i dlatego w tym rozumieniu utrzymanie bezpieczeństwa w zakresie informacyjnym powinno zawierać następujące elementy:[9]

- zwiększanie ochrony własnych systemów informacyjnych;
- stała ocena słabości systemów informacyjnych potencjalnych przeciwników, w tym takie działania jak tworzenie możliwości wtargnięcia do nich przez „tylne drzwi" lub chipping;[10]
- przygotowanie możliwych form odpowiedzi na atak z wykorzystaniem zarówno informacyjnych jak i konwencjonalnych wojskowych środków rażenia;
- rozwijanie metod szacowania poniesionych i / lub zadanych zniszczeń (strat) informacyjnych.

Liberalne podejście do bezpieczeństwa narodowego w aspekcie ochrony systemów informacyjnych polegało będzie na:

- zwiększaniu poziomu powiązań i współzależności systemów informacyjnych różnych państw w celu przeciwdziałania zagrożeniom;
- tworzenie globalnych instytucji i porozumień zapobiegających wojnie informacyjnej.

Wydaje się, że najrozsądniejszym wyjściem godzącym stanowisko liberalne z realistycznym jest tworzenie globalnych instytucji i porozumień przeciwko działaniom wojennym w sferze informacyjnej przy jednoczesnym zwiększaniu świadomości o własnych słabościach i dzięki temu umiejętne podwyższanie poziomu ochrony systemów informacyjnych. Bardzo ciekawą metodę zastosował w tym względzie Izrael. O ile w innych państwach hakerzy są ścigani i wsadzani do więzień to tam, złapani są angażowani do wywiadu w celu wykrywania słabości systemów własnych i poten-

---

[9] *Mathew G. Devost: op. cit.*

[10] *chipping – umieszczanie w sprzedawanym sprzęcie układów elektronicznych, niemożliwych do wykrycia, przeznaczonych do unieruchomienia lub zmodyfikowania działania tego sprzętu na odpowiedni sygnał*

cjalnego przeciwnika. Jak to dosadnie określił, amerykański analityk, Robert Steele: „Jeżeli coś złego dzieje się w systemie to nie jest to łamanie prawa tylko kiepska robota inżynierska. Kiedy my łapiemy hakera to zamiast nauczyć się od niego dajemy mu w zęby podczas gdy w Izraelu złapany haker znajduje zatrudnienie w Mosadzie".

Wojna informacyjna według amerykańskiego Departamentu Obrony to „działania podjęte w celu osiągnięcia informacyjnej przewagi, wspierające narodową strategię militarną, poprzez oddziaływanie na informacje i systemy informacyjne przeciwnika przy jednoczesnej ochronie własnych informacji i systemów informacyjnych". Spotkać się można natomiast również z definicjami wynikającymi z innego podejścia do działań podejmowanych w sieci. John Arquilla i David Ronfeldt[11] identyfikują dwa typy wojny informacyjnej: netwar i cyberwar, określając je w następujący sposób:

- netwar - konflikt pomiędzy społeczeństwami i narodami toczący się na wysokim poziomie i związany z informacjami o nich, w którym próba zniszczenia lub zmodyfikowania informacji jest przeprowadzana w celu zmiany poglądów, o państwie będącym celem ataku, w jego społeczeństwie i otoczeniu;
- cyberwar – określa prowadzenie i przygotowanie do prowadzenia działań militarnych z wykorzystaniem informacji jako podstawowego elementu uzyskania przewagi. Oznacza to utrzymanie równowagi pomiędzy wiedzą i informacją jako naczelnej zasady prowadzenia działań. Powoduje to transformację natury wojny z oddziaływania siłami i środkami rażenia powodującymi istotne i zauważalne straty na zastosowanie środków, niekoniecznie wyrafinowanych technologicznie, ale dzięki swojemu oddziaływaniu przynoszących bardzo konkretne efekty, głównie w sferze psychologicznej ale również materialnej.

Netwar jest rywalizacją idei, w której celem jest informacja, a właściwie wiedza i dlatego wydaje się, że pojęcie to jest blisko związane z określeniem propagandy wojennej (lub wojny propagandowej w zależności od fazy konfliktu). Wśród celów ataków realizowanych w czasie „wojny sieciowej" będą zarówno środki łączności społecznej jak i te realizujące transakcje finansowe, odpowiadające za transport czy też sieci związane z zarządzaniem zasobami energetycznymi. Oczywiście ważne jest niszczenie i ochrona fizycznych środków zapewniających działanie sieci, jednakże

---

[11] *J. Arquilla, D. Ronfeld: Cyberwar is Coming, artykuł dla RAND Corporation*

nacisk kładzie się na niszczenie i obronę przed zniszczeniem najistotniejszych z punktu widzenia nowoczesnego społeczeństwa, związków pomiędzy społeczeństwem a jego państwem rozumianych jako utożsamianie się ze strukturą zapewniającą bezpieczne życie. Oczywistym jest, że działania prowadzone w ramach „wojny sieciowej" będą wymierzone w, bądź realizowane przez kraje o bardzo wysokim stopniu „usieciowienia" (uzależnieniu swoich działań od istnienia sieci teleinformatycznych). Znaczenie tych działań polega na wprowadzeniu stanu dezintegracji pomiędzy państwem i społeczeństwem, utraty zaufania społeczeństwa do możliwości realizowania przez państwo swoich powinności wobec społeczeństwa.

Ta część działań zwana też wojną psychologiczną Martin Libicki[12] podzielił na cztery grupy:

1. działania przeciwko wojskom przeciwnika;
2. działania przeciwko przywódcom przeciwnika;
3. działania wymierzone w wolę narodu przeciwnika do prowadzenia działań;
4. działania narzucające specyficzną kulturę i zachowania narodowi przeciwnika.

Mogą one prowokować kampanie dyplomatyczne, propagandowe czy psychologiczne; polityczne lub kulturalne doprowadzanie do upadku, okłamywanie lub wywieranie wpływu na lokalne media, infiltracja sieci komputerowych i baz danych a także wysiłki w celu wypromowania przy pomocy sieci komputerowych dysydentów i ruchów opozycyjnych.

Zdefiniowane powyżej pojęcie cyberwar będzie z kolei dotyczyło zagadnień związanych z wyznaczeniem sieci teleinformatycznych jako głównego celu działań militarnych (zarówno agresywnych jak i obronnych) w celu uniemożliwienia realizacji innych zadań militarnych. Zmiany zachodzące pod wpływem zastosowania technologii sieciowych we wszystkich organizacjach powodują, że rywalizacja pomiędzy nimi staje się coraz bardziej rywalizacją o jakość tej informacji i jej właściwy przepływ niż tylko posiadanie informacji.

Omówione powyżej aspekty walki informacyjnej mają ścisły związek z walką zbrojną i działaniami militarnymi. Trzeba jednak zauważyć, że procesy globalizacyjne powodują, iż możemy mieć do czynienia z wrogimi działaniami wobec państwa i jego instytucji bez uwzględniania czynnika militarnego. Fakt, że prawo międzynarodowe

---

[12] *M. Libicki: What is Information Warfare?, artykuł dla Institute for National Strategic Studies*

nie nadąża za rozwojem technologii i nie uwzględnia w swojej nomenklaturze wojny w wymiarze cybernetycznym (co zostało omówione w części wstępnej) nie może przesłonić istnienia zagrożeń bezpieczeństwa państw i narodów wynikających z możliwości wykorzystania cyberprzestrzeni jako pola walki. O tym jak ważna jest sprawa ochrony przed tymi zagrożeniami niech świadczy waga jaką przykładają, przodujące pod względem zastosowania technologii teleinformatycznych państwa, do ochrony t.zw. Infrastruktury Krytycznej Państwa (IKP). Pojęcie to jest ściśle związane z potocznym rozumieniem pojęcia infrastruktury, jako zespołu podstawowych urządzeń i instytucji niezbędnych do funkcjonowania gospodarki i państwa. W rozumieniu przeciwdziałania zagrożeniom wieku informacji należy IKP pojmować jako fizyczne i wirtualne systemy o zasadniczym znaczeniu dla możliwości funkcjonowania gospodarki i rządu w minimalnym chociażby zakresie. Jest to ta część infrastruktury państwa, której ciągłość działania jest na tyle ważna dla funkcjonowania państwa, że jej utrata, przerwy w działaniu lub znaczące obniżenie jakości działania może spowodować poważne konsekwencje zagrażające życiu społeczeństwa lub jego pokaźnej części.

Podstawowe elementy wchodzące w jej skład to:

- usługi informacyjne i łączność – składające się z telekomunikacji, dystrybucji i transmisji informacji, sprzętowych i programowych składników sieci danych, itd.;
- sektor finansowy i bankowy – w skład którego zalicza się banki, towarzystwa ubezpieczeniowe, instytucje kredytowe, instytucje nadzoru nad systemem finansowym oraz wszystkie instytucje wspomagające, w tym chroniące systemy obrotu wartościami itd.;
- systemy wodociągowo-kanalizacyjne i dystrybucji żywności - składające się z systemów zapewniających wodę pitną, jej filtrację i transport, usługi związane z dystrybucją żywności, zarządzanie zasobami wody i żywności;
- energetyka – obejmująca elektrownie, linie przesyłowe, sieci transmisyjne i podstacje, system zarządzania energią elektryczną;
- surowce energetyczne – obejmujące ich wydobywanie, magazynowanie i dystrybucję;
- transport – do którego zaliczamy wszystkie składniki służące do transportu ludności i towarów w środowiskach lądowym, morskim i powietrznym;

- służba zdrowia i system ratowniczy – składające się ze służb i instytucji odpowiedzialnych zarówno za działania związane z zachowaniem zdrowia przez społeczeństwo jak również działania w przypadku wystąpienia sytuacji nadzwyczajnych takich jak katastrofy techniczne i naturalne, czy kryzysy społeczne w tym wojny i konflikty;
- władza centralna – a zwłaszcza te jej komponenty, które odpowiadają za obronę narodową, administrację publiczną, opiekę społeczną, porządek publiczny.

Wszystkie składowe systemu Infrastruktury Krytycznej Państwa są ze sobą powiązane a siła ich wzajemnych relacji zależy od wielu czynników, wśród których podstawowymi będą:

- niezależność energetyczna państwa;
- siła gospodarcza rozumiana jako osiągnięty poziom rozwoju gospodarczego;
- poziom rozwoju usług zapewniających bezpieczeństwo socjalne społeczeństwa;
- techniczny i technologiczny rozwój systemów wchodzących w skład IKP;
- nasycenie środkami technologii teleinformatycznych systemów informacyjnych państwa.

Można pokusić się o próbę zdefiniowania macierzy współzależności pomiędzy poszczególnymi elementami IKP.[13] Pokazuje ona (rys. 2.17.), jak ważne dla bezpieczeństwa państwa i pozostałych składowych infrastruktury role pełnią takie jej filary jak energetyka i surowce energetyczne, co jest zrozumiałe i można by rzec tradycyjne oraz łączność i telekomunikacja, która jest systemem nerwowym infrastruktury.

---

[13] *R. Gogela, L. Novàk, A. Šefčik: Critical Infrastructure Modelling, w Security and Protection of Information 2003,*

	usługi informacyjne i łączność	finanse i bankowość	wodociągi i dystrybucja żywności	energetyka	surowce energetyczne	transport	służba zdrowia i system ratowniczy	władza centralna
usługi informacyjne i łączność	–	M	L	H	M	L	M	M
finanse i bankowość	H	–	L	H	M	M	L	M
wodociągi i dystrybucja żywności	M	M	–	H	M	H	M	L
energetyka	H	M	M	–	H	M	M	M
surowce energetyczne	H	M	M	H	–	H	M	M
transport	H	M	L	H	H	–	L	M
służba zdrowia i system ratowniczy	H	M	M	H	H	H	–	M
władza centralna	H	M	L	H	H	M	M	–

Rysunek 2.17. Macierz współzależności sektorów infrastruktury krytycznej (H – duża, M – średnia, L – niska)

Sposób ochrony tej części żywotnych zasobów państwa musi być różny w państwach o diametralnie różniących się systemach prawnych i gospodarczych, jak np. Polski i USA. Pewne, dość istotne, zapóźnienie technologiczne naszego kraju w stosunku do Stanów Zjednoczonych, niekwestionowanego lidera w wykorzystaniu technologii informacyjnych oraz fakt znacznego jeszcze sektora państwowego w gospodarce nakłada szczególną rolę na organy administracji państwa w przygotowaniu i prowadzeniu ochrony Infrastruktury Krytycznej Państwa.

Niezależnie jednak od wspomnianych wyżej uwarunkowań w każdym państwie można wyróżnić następujące pola administrowania:

- prywatny, gdzie mamy do czynienia z prywatną odpowiedzialnością za sprawy domu i rodziny;
- municypalny (samorządowy), w którym lokalne władze samorządowe, małe organizacje i firmy administrują i wpływają na działalność niewielkich obszarów;
- regionalny, gdzie wpływ administracji, średnich organizacji i firm rozciąga się na znacznym obszarze;
- państwowy, w którym mamy do czynienia z administrowaniem całym krajem a swój wpływ poza administracją państwową wywierają również duże organizacje i firmy;
- międzynarodowy, gdzie bardzo duży jest wpływ relacji międzynarodowych i międzypaństwowych; wielkich, światowych, ponadnarodowych organizacji i firm i ich zależność od składowych infrastruktury (rys.2.18.).[14]

Trzecim wymiarem tak skonstruowanego warstwowego modelu infrastruktury krytycznej jest obszar zarządzania podzielony na pola zarządzania:

- społecznego, oznaczającego realizację zadań społecznych, politycznych i gospodarczych wywierających wpływ na społeczeństwo i jakość życia ludzi;
- organizacyjnego, określającego działania polityczne i gospodarcze, strategie, struktury, regulacje prawne i inne przedsięwzięcia związane z IKP;
- informacyjnego, rozumianego jako system informacyjny, wspomagający całość infrastruktury;
- aplikacyjnego, realizowanego dla pojedynczego kompleksu funkcjonalnego jako podstawowego elementu wykonawczego wspomagającego część usług infrastruktury krytycznej;
- technologicznego, reprezentującego komponenty technologiczne (oprogramowanie, sprzęt itd.) i ich integrację w podstawowe bloki funkcjonalne;
- standaryzacyjnego, będącego wspólnym polem służącym do opisu cech środowiska zarówno naturalnego jak i stworzonego przez człowieka - charakterystyki ilościowo – jakościowe.

---

[14] *ibidem*

SEKTOR ADMINSTRACJI / FILAR INFRASTRUKTURY KRYTYCZNEJ	prywatny	samorządowy	regionalny	państwowy	międzynarodowy
usługi informacyjne i łączność	M	H	H	H	M
finanse i bankowość	L	M	M	H	M
wodociągi i dystrybucja żywności	M	H	M	M	L
energetyka	L	M	H	H	L
surowce energetyczne	M	M	M	H	H
transport	M	H	H	M	L
służba zdrowia i system ratowniczy	M	H	H	M	M
władza centralna	L	M	H	H	M

Rysunek 2.18. Tablica zależności sektorów administrowania od filarów infrastruktury krytycznej.

Podstawowymi, strategicznymi celami ochrony informatycznego komponentu IKP powinno być:

- zapobieganie cyberatakom na IKP;
- zredukowanie podatności IKP na zagrożenia płynące z cyberprzestrzeni;
- minimalizowanie zniszczeń poniesionych na skutek cyberataków i minimalizowanie czasu niezbędnego na odtworzenie.

Przywołując przykład Stanów Zjednoczonych należy powiedzieć, że powołany przez prezydenta Busha Departament do spraw Bezpieczeństwa Kraju (Department of Homeland Security - DHS) skupiający 22 instytucje odpowiedzialne za bezpieczeństwo państwa realizuje również bardzo ważne zadania związane z bezpieczeństwem cyberprzestrzeni.

Należą do nich:[15]

- tworzenie i rozwijanie dalekosiężnego planu ochrony kluczowych zasobów i infrastruktury krytycznej;
- zarządzanie kryzysowe w przypadku wystąpienia ataku na IKP;
- wsparcie techniczne dla prywatnych i państwowych organizacji dotkniętych atakiem na infrastrukturę krytyczną, zgodnie z planami bezpieczeństwa;

[15] *The National Strategy to Secure Cyberspace, Washington DC, 2003*

- koordynacja z innymi agencjami rządowymi przedsięwzięć ostrzegawczych, zabezpieczających i przeciwdziałających zagrożeniom;
- kreowanie i finansowe wspieranie badań naukowych i wdrażania nowych rozwiązań zwiększających bezpieczeństwo państwa.

W tym celu przygotowano strategię, która oparta jest na realizacji przedsięwzięć ujętych w pięć priorytetów:

1. System reagowania, którego zadaniem jest szybkie wykrywanie i identyfikacja zagrożeń (ataków), wymiana informacji z innymi elementami systemu ochrony IKP i znajdowanie środków zaradczych poprzez realizowanie następujących działań:
   a. ustanowienie publiczno – prywatnej architektury mogącej przeciwdziałać incydentom w cyberprzestrzeni;
   b. prowadzenie taktycznych i strategicznych analiz cyberataków i szacowanie podatności na nie;
   c. wzmacnianie rozwoju przez sektor prywatny możliwości śledzenia stanu bezpieczeństwa cyberprzestrzeni;
   d. rozwijanie systemu wczesnego ostrzegania i informowania o zagrożeniach w sieci w celu wspomożenia roli DHS w koordynowaniu zarządzania kryzysowego bezpieczeństwem cyberprzestrzeni;
   e. poprawianie narodowego zarządzania w przypadku wystąpienia incydentów;
   f. koordynowanie procesu dobrowolnego współuczestnictwa w rozwijaniu planu zapewnienia ciągłości działania;
   g. sprawdzanie planów ciągłości działania dla systemów państwowych;
   h. poprawianie i rozszerzanie wymiany informacji o atakach, zagrożeniach i podatnościach pomiędzy instytucjami państwowymi i prywatnymi.

   Przedsięwzięcia te nie wymagają realizacji drogich państwowych programów i rozbudowanej biurokracji. Chodzi o takie zintegrowanie posiadanych przez sektory prywatny i państwowy zasobów, żeby uzyskać efekt synergii w realizowaniu zadań: analizy, ostrzegania, zarządzania kryzysowego, odpowiedzi i odzyskiwania utraconych zasobów.
2. Program redukcji zagrożeń i podatności na nie, który poprzez wskazanie słabych punktów w zabezpieczeniach infrastruktury krytycznej ma doprowadzić do ich wyeliminowania. Program ten realizowany jest przez następujące działania:

a. rozwijanie prawnych możliwości przeciwdziałania i zaskarżania działań szkodliwych z wykorzystaniem cyberprzestrzeni;
b. kreowanie procesu lepszego zrozumienia potencjalnych konsekwencji istnienia zagrożeń i podatności na nie;
c. ochrona mechanizmów Internetu poprzez poprawianie protokołów i sposobów przesyłu informacji;
d. promowanie zaufanych systemów kontroli, nadzoru i pozyskiwania danych,
e. redukcja i zapobieganie słabym punktom oprogramowania;
f. zrozumienie współzależności między elementami infrastruktury i poprawa ochrony fizycznej systemów informatycznych i telekomunikacyjnych;
g. określanie ważności badań naukowych i wdrożeń z dziedziny bezpieczeństwa informacyjnego prowadzonych przez agendy państwa;
h. ocena i ochrona tworzonych systemów.

3. Program zwiększania świadomości zagrożeń i szkolenia jako metoda pozwalająca na zmniejszenie możliwości zaatakowania systemu infrastruktury krytycznej, realizowana poprzez następujące działania:
   a. promowanie świadomości konieczności ochrony swojej własnej części cyberprzestrzeni w celu zwiększenia bezpieczeństwa państwa;
   b. propagowanie właściwych programów szkolenia i nauczania dla zabezpieczenia potrzeb bezpieczeństwa narodowego w zakresie bezpieczeństwa informacyjnego;
   c. zwiększanie skuteczności istniejących państwowych programów szkoleń;
   d. promowanie pomocy dla sektora prywatnego w zdobywaniu ogólnie uznawanych poświadczeń znajomości zagadnień związanych z bezpieczeństwem informacyjnym.
4. Ochrona cyberprzestrzeni instytucji rządowych realizowana poprzez:
   a. ciągłą ocenę zagrożeń i słabości systemów państwowych;
   b. legalizowanie i autoryzowanie użytkowników państwowych systemów informatycznych;
   c. ochrona bezprzewodowych lokalnych sieci państwowych;
   d. poprawianie ochrony działań realizowanych na zlecenie rządu;
   e. wzmacnianie władz lokalnych do ustanawiania i realizowania programów ochrony informacji oraz uczestniczenia w wymianie informacji i analiz z instytucjami szczebla państwowego.

5. Współpraca krajowa i międzynarodowa w ochronie cyberprzestrzeni, jako element mogący zmniejszyć zagrożenia wynikające z globalnego charakteru cyberprzestrzeni. Należy ją rozwijać realizując następujące przedsięwzięcia:
   a. wzmocnienie działań kontrwywiadowczych w cyberprzestrzeni;
   b. zwiększenie możliwości ataku i odwetu;
   c. poprawienie koordynacji odpowiedzi na atak z wewnętrznego, krajowego systemu bezpieczeństwa;
   d. współpraca z przemysłowymi i międzynarodowymi organizacjami w celu ułatwienia dialogu i partnerstwa państwowych i prywatnych sektorów nastawionych na ochronę infrastruktury informacyjnej i promowanie światowej „kultury bezpieczeństwa";
   e. stworzenie narodowej i międzynarodowej sieci śledząco - ostrzegającej wykrywającej i przeciwdziałającej cyberatakom w momencie ich pojawienia się;
   f. zachęcanie innych krajów do przyłączenia się do Konwencji o Cyberprzestępczości przyjętej przez Radę Europy lub upewnienie się, że ich prawo i procedury są co najmniej odpowiednie do tej konwencji.

Opisane powyżej amerykańskie podejście do ochrony Infrastruktury Krytycznej Państwa może być przykładem wniosków jakie wyciągają kraje o bardzo zaawansowanym poziomie rozwoju sieci i systemów telekomunikacyjnych w obliczu zagrożeń okresu po zakończeniu zimnej wojny a jednocześnie okresu, w którym obserwujemy coraz większy wzrost zagrożeń związanych z terroryzmem, którego metody działań w dobie globalizacji stają się również globalne i wykorzystują zdobycze nowoczesnych technologii. Ważne zatem stają się działania, nie tylko w sferze praktycznych rozwiązań pozwalających na zwiększenie bezpieczeństwa w cyberprzestrzeni, ale również w sferze badań naukowych pozwalających z jednej strony opisać rzeczywistość globalnego systemu informacyjnego z drugiej zaś znajdować rozwiązania zadań wynikających z konieczności ochrony tego systemu przed istniejącymi zagrożeniami. Podobnie jak w wielu innych badaniach systemów rzeczywistych tak i tutaj nasuwa się potrzeba wykorzystania metody modelowania systemów jako najwłaściwszej do poznawania i rozwiązywania problemów aktualnych i przyszłych. Przykładem takich działań są przedstawione na rysunkach 2.17 i 2.18 próby stworzenia warstwowego modelu Infrastruktury Krytycznej Państwa jako tej części infrastruktury, która decyduje o bezpieczeństwie państwa.

2.4.3. *Wojna informacyjna elementem wojny „tradycyjnej"*

Mówiąc o działaniach powiązanych z informacjami musimy również rozróżnić działania wojenne wieku informacyjnego od informacyjnych działań wojennych. Spowodowane jest to tym, że bardzo często zamiennie stosuje się te pojęcia mimo tego, że pierwsze z nich określa wysoki stopień nasycenia technologiami informacyjnym a drugi uznanie informacji jako osobnej sfery działań, potencjalną bronią i istotnym celem, co oznacza, że działania te nie zależą od technologii aczkolwiek nowoczesne technologie zwiększają możliwości realizacji tych działań.[16]

W tym rozumieniu każda akcja skierowana przeciwko informacjom (i urządzeniom im służącym, jak np. zniszczenie centrali telefonicznej) będzie wojennym działaniem informacyjnym. Również każde działanie podjęte w celu obrony informacji (np. ochrona antywirusowa) jest działaniem wchodzącym w skład Information Warfare.

Uogólniając, informacyjne działania wojenne dotyczą: eksploatacji, niszczenia, zmiany oraz ochrony informacji i obejmują takie tradycyjne środki jak:

1. operacje psychologiczne – rozumiane jako użycie informacji do wpływania na sposób działania przeciwnika;
2. walkę elektroniczną – powodującą blokowanie dopływu ważnych dla nieprzyjaciela informacji;
3. maskowanie wojskowe – wprowadzające przeciwnika w błąd co do naszych możliwości i intencji;
4. fizyczne niszczenie – poprzez zamianę zmagazynowanej energii w niszczącą siłę począwszy od bomb konwencjonalnych na bombach elektromagnetycznych kończąc;
5. środki ochronne – uniemożliwiające nieprzyjacielowi poznanie naszych możliwości i intencji;
6. atak informacyjny – bezpośrednio niszczący informację bez widocznych zmian w fizycznych urządzeniach, w których się znajdowały.

Wszystkie te sposoby oddziaływania na informacje można podzielić na pośrednie i bezpośrednie. Pierwsze z nich mają za zadanie wykreowanie takiej rzeczywistości w świadomości nieprzyjaciela jaka jest dla nas najlepsza a drugie taką zmia-

---

[16] *Gen. Ronald R. Fogelman: Cornerstones of Information Warfare*

nę informacji posiadanych przez niego aby był przekonany, o swojej wiedzy. Przykładem pierwszych może być tworzenie fikcyjnych stanowisk dowodzenia dla zmylenia rozpoznania przeciwnika a drugich wprowadzenie do jego bazy danych informacji o nieistniejących zgrupowaniach wojsk.

„Information Warfare to wszelkie działania podejmowane przez rządy, grupy lub pojedyncze osoby, w celu zdobycia dostępu do systemów informacyjnych innych krajów ... a także działania podjęte w celu ochrony przed tym dostępem".[17] Taka definicja jest z pewnością zbyt szeroka, ponieważ obejmuje również działania, które z założenia miały być psotą, czy też próbą sprawdzenia swoich umiejętności w przełamywaniu zabezpieczeń. Przyjęcie jej jako obowiązującej mogłoby spowodować, że należy rozpocząć działania odwetowe nawet przy zaistnieniu przypadkowego lub zamierzonego działania młodocianego hakera. Dlatego też bardziej precyzyjna i oddająca wojenny w rozumieniu prawa międzynarodowego charakter działań będzie definicja mówiąca o tym, że jest to „zastosowanie, na wielką skalę, sił destrukcyjnych przeciwko informacyjnym środkom i systemom, przeciwko komputerom i sieciom wspomagającym cztery filary infrastruktury (energetykę, łączność, finanse i bankowość oraz transport)"[18]. Wojna jako sposób realizowania polityki w wieku informacyjnym może stać się zupełnie nową jakością. Łatwiej będzie zaakceptować, szczególnie w czasach kiedy wojny są na żywo transmitowane przez telewizje, zniszczenie nieprzyjacielskiej struktury informacyjnej, co skutkuje stratami, również w ludziach, ale w zdecydowanej większości niekoniecznie kojarzonymi z oddziaływaniem na zasoby informacyjne, niż bombardowanie, którego niszczące efekty są widoczne natychmiast a ofiary wyglądają bardziej spektakularnie.

Wśród środków walki informacyjnej znaleźć można, podobnie jak i wśród tradycyjnych, konwencjonalnych środki ofensywne i defensywne. Do ofensywnych należą:

- wirusy komputerowe, wprowadzone do nieprzyjacielskich komputerów poprzez wykonanie ataków lub poprzez osoby „przekonane" do takiego działania;
- bomby logiczne, czyli taki rodzaj wirusów, które zainstalowane w komputerach i sieciach nieprzyjacielskich mogą przez długie lata pozostawać

---

[17] *Raport Komisji Browna*
[18] *Brian C. Lewis: Information Warfare*

w stanie uśpienia, aby na odpowiedni sygnał przystąpić do swych niszczycielskich działań;

- „chipping" - metoda (najprawdopodobniej stworzona przez CIA) polegająca na montowaniu do sprzedawanego sprzętu mikroukładów elektronicznych, które uaktywniają się na sygnał zakłócając lub uniemożliwiając pracę systemów;
- robaki – samopowielające się programy, które zajmują coraz większe zasoby systemu, aż do jego całkowitego unieruchomienia;
- konie trojańskie – wrogi kod dołączony do legalnego oprogramowania w celu realizacji nielegalnych funkcji;
- tylne drzwi – mechanizm wbudowany przez twórców oprogramowania w celu umożliwienia dostania się do atakowanego systemu bez wiedzy jego właściciela
- urządzenia trwale lub czasowo niszczące sprzęt lub nośniki informacji:
  - tradycyjne środki walki;
  - urządzenia do niszczenia elektromagnetycznego:
    - broń mikrofalowa wysokiej mocy – High Power Microwave – generująca elektromagnetyczny sygnał wielkiej mocy (rzędu gigawatów) o radiowej częstotliwości;
    - broń o szerokim zakresie częstotliwości – Ultra Wide Band – generująca elektromagnetyczny sygnał dużej mocy na różnych zakresach częstotliwości;
    - broń wysokiej energii radiowej częstotliwości – High Energy Radio Frequency – jak HPM;
    - urządzenia generujące impuls elektromagnetyczny – Electromagnetic Pulse – które wybuchając w pobliżu atakowanych urządzeń systemu informatycznego, generują impuls elektromagnetyczny niszczący znajdujące się w pobliżu urządzenia elektroniczne.

Środkami defensywnymi będą natomiast wszelkie działania zmierzające do zabezpieczenia swoich systemów informacyjnych przed penetracją potencjalnego przeciwnika.

Działania te będą obejmowały przedsięwzięcia w takich aspektach ochrony jak, zapewnienie bezpieczeństwa:

a. fizycznego – poprzez stworzenie właściwych warunków do umiejscowienia urządzeń służących do zbierania, przetwarzania i dystrybucji danych; będzie to dotyczyło przeciwdziałania zagrożeniom celowym jak i naturalnym;
b. elektromagnetycznego – przyjmując takie rozwiązania techniczne i organizacyjne, które zabezpieczą systemy teleinformatyczne przed możliwością penetracji poprzez rejestrowanie promieniowania elektromagnetycznego chronionych elementów systemów teleinformatycznych i jednocześnie zabezpieczą ich newralgiczne punkty przed możliwością oddziaływania bronią elektromagnetyczną;
c. kryptograficznego – pozwalającego na porozumiewanie się poszczególnych elementów systemu bez obawy o podsłuchanie, a więc stosowanie takich systemów szyfrowania i deszyfracji informacji, które będąc nieskomplikowane i nie powodując opóźnień dla własnych elementów systemu są jednocześnie niemożliwe do rozszyfrowania i / lub zakłócenia dla przeciwnika;
d. dostępu do urządzeń – a więc stworzenia takiego systemu dostępu do miejsc, w których znajdują się najistotniejsze elementy systemu, aby niemożliwe było dotarcie do nich osobom nieupoważnionym, które mogłyby dokonać aktu sabotażu, zamontowania urządzeń zakłócających pracę systemu bądź rozpoznać rozwiązania techniczne służące zabezpieczeniu chronionych systemów.

Zdobywanie aktualnych i dokładnych danych, ich szybka i właściwa analiza oraz terminowa, niezakłócona dystrybucja są jednymi z najważniejszych czynników warunkujących powodzenie na polu walki. Każdy dowódca, aby podjąć właściwą decyzję musi umieć odpowiedzieć sobie na następujące pytania:

– co się dzieje ?
– co to oznacza ?
– co należy zrobić ?

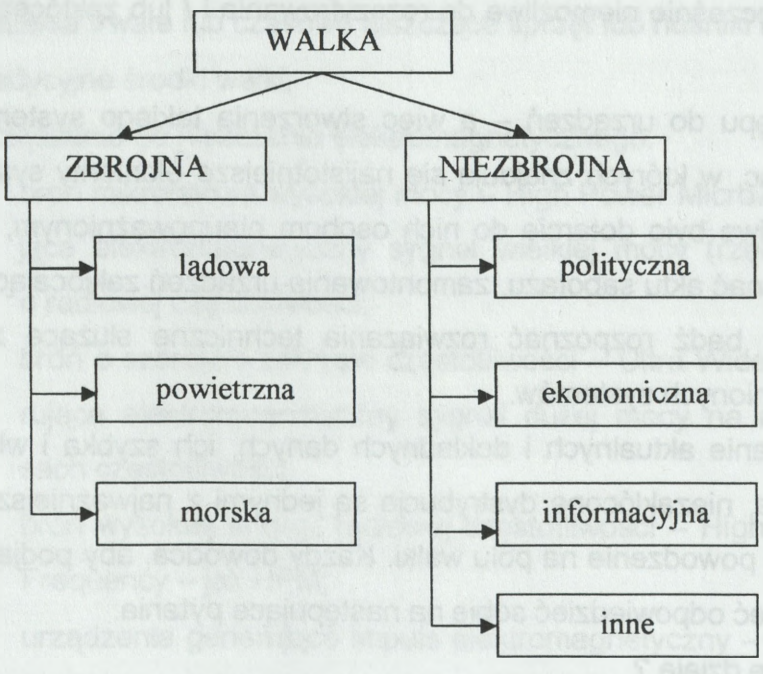
Dzisiejsze technologie informacyjne umożliwiają zbieranie, gromadzenie i przetwarzanie danych, ich dystrybucję oraz zobrazowanie sytuacji na polu walki w czasie zbliżonym do rzeczywistego.

„Musicie mieć możliwość komunikowania się ze swoimi siłami i wymiany informacji w dowolnym momencie i z dowolną częstotliwością. Poza tym musicie mieć możliwość robienia tego w skali globalnej. Jedną sprawą jest posiadanie odpowied-

nio wysokiego poziomu technologii i techniki oraz odpowiednio przygotowanego systemu zbierania informacji zarówno w przestrzeni kosmicznej, jak i na lądzie i w morzu drugą natomiast umiejętność jej wykorzystania we właściwym czasie."[19] Te słowa jednego z wysokich dowódców armii Stanów Zjednoczonych wyraźnie wskazują na konieczność umiejętności wykorzystania informacji często zdobytych dużym nakładem sił i środków.

Zgodnie z obowiązującymi w Polsce poglądami walka informacyjna to jeden z niezbrojnych sposobów prowadzenia walki, będący „kooperacją negatywną, wzajemną, realizowaną w sferach: zdobywania informacji (rozpoznania), zakłócania informacyjnego i obrony informacyjnej."[20]

Miejsce walki informacyjnej wśród innych rodzajów walki przedstawia rysunek 2.19.



Rysunek 2.19. Miejsce walki informacyjnej w ogólnej przestrzeni walk[21]

W przypadku walki zbrojnej podstawą sukcesu jest zawsze precyzja rażenia i czas reakcji ogniowej. Przy porównywalnych ilościowo i jakościowo stanach uzbro-

---

[19] *Gen. Ronald R. Fogelman, Szef Sztabu Sił Powietrznych USA w mowie wygłoszonej do Stowarzyszenia Łączności i Elektroniki Sił Zbrojnych USA, 25.04.1995, Information Operations: The Fifth Dimension of Warfare*

[20] *Regulamin działań wojsk lądowych, Warszawa, 1999*

[21] *na podstawie G. Nowacki Współczesne poglądy na prowadzenie walki informacyjnej, AON, Warszawa 2001*

jenia zwycięstwo będzie po stronie, która szybciej i precyzyjniej razi przeciwnika. Wynika z tego, że optymalne prowadzenie walki zbrojnej musi się opierać na właściwym wykorzystaniu siły rażenia wojsk poprzez stwarzanie warunków do osiągania jak najwyższej precyzji ognia i jednocześnie do minimalizowania czasu reakcji w tym zakresie. Niedoskonałości w tym zakresie muszą być rekompensowane masą ognia oraz większą liczbą posiadanych sił i środków walki. Stworzenie warunków do uzyskania optymalnej precyzji rażenia i minimalizacji czasu reakcji to zadania realizowane w ramach walki informacyjnej. Rozpoznanie, pozwala na właściwą lokalizację celów rażenia, dając jednocześnie informacje o jego zamiarach a zakłócanie informacyjne i obrona informacyjna pozwalają na wyprzedzenie działań przeciwnika i wprowadzenie go w błąd co do naszych zamiarów.

Określone powyżej elementy walki informacyjnej:

- rozpoznanie;
- zakłócanie;
- obrona informacyjna;

stanowią istotę walki informacyjnej. Z tych trzech komponentów fundamentalny charakter ma rozpoznanie, definiowane jako:[22]

- wiedza dotycząca działalności i możliwości prowadzenia walki przez aktualnego lub potencjalnego przeciwnika, obszaru prowadzenia działań oraz warunków atmosferycznych i klimatycznych;
- zespół sił i środków przeznaczonych do zdobywania i gromadzenia informacji, przetwarzania ich w dane rozpoznawcze oraz rozpowszechniania tych danych do sztabów i wojsk w układzie narodowym i sojuszniczym.

Zadania związane z pozyskiwaniem informacji mogą być realizowane w formie bezpośredniej (rozpoznanie osobowe) jak i pośredniej, technicznej. Pierwsza z tych form realizowana może być poprzez rozpoznanie agenturalne, patrolowe bądź specjalne lub kombinację tych działań. Natomiast techniczna forma zdobywania informacji może mieć wieloraką postać:

1. Rozpoznanie elektromagnetyczne – polegające na zdobywaniu informacji na podstawie emisji elektromagnetycznej systemów elektronicznych przeciwnika. Dzieli się ono na rozpoznanie:

---

[22] *Rozpoznanie wojskowe, Szt. Gen. WP 1531/2001*

- radiowe – gdzie nośnikiem informacji są fale elektromagnetyczne wykorzystywane przez radiostacje KF – UKF, środki łączności satelitarnej, radioliniowej i inne;
- radiolokacyjne – w którym stacje radiolokacyjne wykrywają powietrzne, naziemne i nawodne cele ruchome i nieruchome; możemy mieć tu do czynienia z systemami:
  - rozpoznania obszaru powietrznego;
  - nadzorowania pola walki;
  - kierowania ogniem;
  - obrony przeciwlotniczej;
  - rozpoznania powierzchni ziemi;
  - optoelektroniczne – wykorzystujące informacje dostarczane przez fale pasma optycznego (ultrafioletowe, widzialne i podczerwone) a wykorzystywane przez urządzenia: telewizyjne, termowizyjne, noktowizyjne i laserowe.

2. Rozpoznanie czujnikowe – polegające na obserwacji stanów w środowisku akustycznym, elektrycznym, magnetycznym i chemicznym.
3. Rozpoznanie informatyczne – które polega na zdobywaniu informacji znajdujących się w systemach teleinformatycznych przeciwnika.

Działania wchodzące w skład zakłócania informacyjnego mają charakter przeciwstawny rozpoznaniu i realizowane są przez siły i środki walki radioelektronicznej, działania psychologiczne, specjalne a także bezpośrednio przez wojska uczestniczące w walce. Mają one na celu niedopuszczenie do wykorzystywania przez przeciwnika spektrum elektromagnetycznego co doprowadzi do obniżenia jego efektywności funkcjonalnej. Wykorzystując różne techniki można zniszczyć lub uniemożliwić pracę źródłom zdobywania danych, przetwornikom danych i sygnałów oraz układom odbierającym a także zmieniać strukturę nośników danych i sygnałów. Rezultatem zakłócania informacyjnego powinno być zniekształcenie obrazu pola walki poprzez ograniczenie napływu danych prawdziwych z pola walki.

Działania wchodzące w skład zakłócania informacyjnego można również podzielić na:

- bezpośrednie, osobowe – polegające na oddziaływaniu na układ recepcyjny człowieka realizowane poprzez:

- pozorowanie (wprowadzanie w błąd),
- działania psychologiczne;
- pośrednie, techniczne – których celem są urządzenia pośredniczące w zdobywaniu, przetwarzaniu i przekazywaniu informacji i dzielące się ze względu na środowisko zakłócania na:
  - elektromagnetyczne, dzielące się względu na wykorzystywane pasma częstotliwości na:
    - radiowe;
    - radiolokacyjne;
    - optoelektroniczne;
    - czujnikowe;
    - informatyczne.

Zarówno pośrednie jak i bezpośrednie działania zakłócające mają na celu wprowadzenia przeciwnika w błąd co do naszych intencji i możliwości działania jak i zachwiania zaufania do własnej zdolności do prowadzenia działań bojowych. O ile działania prowadzone z wykorzystaniem metod technicznych są stosunkowo łatwe do zidentyfikowania (co nie oznacza możliwości przeciwdziałania), to działania w sferze percepcji czy psyche mogą zostać przez dłuższy czas niezauważone i być lekceważone. Istotą pozorowania jest bowiem stwarzanie wrażenia prawdy tam gdzie jej nie ma, natomiast działania psychologiczne wspierając pozorowanie mogą też realizować takie cele jak:

- załamanie morale oraz zdolności bojowej wojsk przeciwnika oraz sprzyjającej im ludności i organizacji państwa wrogiego;
- podniesienie morale wojsk własnych i ludności im sprzyjającej;
- współudział w skutecznym maskowaniu wojsk własnych;
- kształtowanie niekorzystnej, do prowadzenia przez przeciwnika działań bojowych, sytuacji politycznej i militarnej zarówno na arenie stosunków dwustronnych jak i wielostronnych ze szczególnym uwzględnieniem organizacji ponadnarodowych;
- stwarzanie, w sferze pozamilitarnej, warunków mających wpływ na pomyślną realizację własnych działań wojskowych;
- bezpośrednie wspieranie działań wojsk własnych.

Działania te stają się niezwykle efektywne szczególnie w dobie powszechnej globalizacji. Ich najczęściej bezkrwawy skutek wskazuje drogę rozwiązywania konfliktów bez potrzeby uciekania się do użycia siły militarnej.

Kolejnym sposobem prowadzenia walki informacyjnej jest obrona informacyjna. Jest to ta forma działań, której celem jest uniemożliwienie bądź ograniczenie możliwości niepowołanego dostępu do informacji, które odzwierciedlają lub mogą ukazać stan faktyczny, usytuowanie i zamiary działania wojsk własnych czy ochronę własnych procedur dowodzenia wojskami i kierowania środkami walki przed zakłóceniem informacyjnym stosowanym przez przeciwnika. Przedsięwzięcia te realizują bezpośredni użytkownicy systemów informacyjnych w ramach zabezpieczenia bojowego.[23] Podobnie jak zakłócanie tak i obrona informacyjna ma swoją formę osobową, bezpośrednią i pośrednią, techniczną.

W skład tej pierwszej wchodzą działania związane z:

- obroną psychologiczną;
- kontrwywiadem;
- ukrywaniem.

Mają one na celu: niedopuszczenie do sytuacji, w której człowiek traci wolę walki i poddaje się depresji, zapobieganie obcej działalności wywiadowczej i ukrywanie wojsk własnych.

Informacyjna obrona techniczna polega na niedopuszczeniu do rozpoznania i zakłócenia środków i urządzeń wojsk własnych. Wyróżnia się tu następujące sposoby obrony:

a. elektromagnetyczną;
b. czujnikową;
c. informatyczną;
d. maskowanie.

Pierwsza z tych obron jest reakcją na istnienia rozpoznania i zakłócania fal elektromagnetycznych. Druga sprowadza się do ochrony przed rozpoznaniem i zakłócaniem własnych detektorów. Obrona informatyczna realizuje zadania związane z istnieniem zagrożeń dla systemów i sieci teleinformatycznych związanych zarówno z możliwością wprowadzenia do systemu oprogramowania złośliwego jak i innych metod i sposobów zagrażania informacjom w nich przetwarzanym. Realizuje się

---

[23] *K. Ćwiklik: Analiza systemowa zjawiska wojny informacyjnej, AON Warszawa, 2003*

tu szereg działań począwszy od stworzenia procedur właściwego, bezpiecznego używania komputerów aż po wyrafinowane rozwiązania sprzętowo – programowe zapewniające bezpieczeństwo informacyjne. Maskowanie ma coraz większe znaczenie ze względu na pojawienie się bardzo precyzyjnych środków rażenia. Ta forma działań obronnych ma na celu uniemożliwienie przeciwnikowi zebrania informacji na temat obiektów mogących stać się celem uderzeń.

Fakt, że w sposób w miarę precyzyjny jesteśmy w stanie wyspecyfikować sposoby prowadzenia walki informacyjnej w sferze militarnej jest dobrym prognostykiem co do możliwości formalnego opisania działań Information Warfare w całym obszarze cyberprzestrzeni.

2.4.4. Modelowanie walki informacyjnej

Jak widać z dotychczasowych rozważań istnieje kilka warstw, które należy brać pod uwagę w modelowaniu zagadnień związanych z wojną informacyjną:

- prawna – kodyfikująca zjawiska związane z działalnością w cyberprzestrzeni;
- społeczna – opisująca wpływ działań w cyberprzestrzeni na realizację życiowych procesów społecznych w tym sprawne zarządzanie państwem ale również na prowadzenie działań militarnych;
- organizacyjno – techniczna – opisująca zagrożenia i środki zaradcze.

Pierwsza z tych płaszczyzn pozostaje ciągle jeszcze daleko w tyle za rozwojem technologii. Jak pokazano w pierwszym podrozdziale w prawie międzynarodowym istnieje bardzo wiele niejasności interpretacyjnych dotyczących pojęcia wojny informacyjnej. O ile w dokumentach doktrynalnych opisujących działania wojenne wieku informacyjnego ale również działania wojny informacyjnej w jej aspekcie wojskowym można zidentyfikować zachowania systemu, które można przetransponować do postaci modelu o tyle sfera cywilnych oddziaływań wydaje się wciąż jeszcze mało skodyfikowana a przez to trudna do opisu. Tym niemniej fakt braku wspomnianych wyżej rozwiązań legislacyjnych nie może być powodem do zaniechania prowadzenia takich badań.

Przedstawiony powyżej warstwowy model Infrastruktury Krytycznej Państwa oraz wyspecyfikowane za amerykańską strategią ochrony cyberprzestrzeni działania prowadzące do zapewnienia bezpieczeństwa są wystarczającą podstawą do podjęcia pogłębionych studiów nad możliwościami modelowania walki informacyjnej i ana-

lizy jej wpływu na bezpieczeństwo państwa. Wydaje się, że stosunkowo najlepiej zidentyfikowanym, co nie oznacza, że do końca rozpoznanym, obszarem walki informacyjnej jest ten, który wchodzi w skład działań militarnych. Działania związane z prowadzeniem walki elektronicznej czy niszczeniem fizycznym niejednokrotnie były przedmiotem modelowania w ramach prac prowadzonych nad odzwierciedleniem procesów zachodzących na polu walki natomiast takie elementy operacji informacyjnych jak operacje psychologiczne czy informowanie opinii publicznej ciągle jeszcze pozostają poza obszarem dogłębnych analiz pozwalających na stworzenie ich postaci modelowych. Wynika to z pewnością z wielkiego stopnia skomplikowania zarówno celu tych oddziaływań, którym są zarówno pojedynczy ludzie jak i zbiorowiska (grupy) ludzkie jak i olbrzymich możliwości realizowania tych działań.

Płaszczyzna organizacyjno – techniczna to umiejętność zidentyfikowania tych cech systemów informacyjnych, które decydują o możliwości zaistnienia zagrożenia z technikami przeciwdziałania im. Istnieje wiele cech systemów informacyjnych, które powodują, że są one w mniejszym lub większym stopniu narażone na oddziaływanie zagrożeń. Wśród różnego rodzaju klasyfikacji szczególnie wyróżnia się jedna, która daje podstawy do rozwiązania problematyki modelowania aspektów technicznych i technologicznych walki informacyjnej. DARPA[24] specyfikuje zagrożenia dla infrastruktury zgrupowane w pięciu kategoriach:

1. Zewnętrzny atak pasywny – podsłuchiwanie, analiza emisji ujawniającej, analiza sygnałów, analiza ruchu w sieci.
2. Zewnętrzny atak aktywny – zamiana lub wstawienie, zagłuszanie (zakłócanie), przepełnienie, podszywanie się.
3. Ataki przeciwko działaniu systemu – kryptoanaliza.
4. Wewnętrzne ataki – kradzież usług, kradzież danych.
5. Atak połączony z dostępem i modyfikacją systemu – łamanie zabezpieczeń, omijanie zezwoleń, manipulowanie.

Te zagrożenia mają różne odzwierciedlenie w stosowanych metodach i celach ataków. Istotne z punktu zrozumienia zagrożeń jest zidentyfikowanie cech systemu, które pozwalają na zaistnienie zagrożeń. Będą one określały podatność systemu na oddziaływanie zagrożeń a jednocześnie świadomość ta pozwoli na dobranie takich technik ochrony zasobów, które pozwolą przeciwdziałać możliwości ingerencji w cha-

---

[24] *The Defense Advanced Research Projects Agency – agencja zajmująca się rozwojem najnowszych technologii i ich zastosowań w dziedzinie obronności*

rakterystyki systemów. Przedstawiona poniżej tabela określa możliwości zastosowania technik ochrony w zależności od źródeł podatności na zagrożenia.[25] Zastosowano w niej oznaczenia określające czy i w jakim zakresie możliwe jest zastosowanie określonych technik do usunięcia bądź zmniejszenia podatności systemu na zagrożenia.

	przeznaczone bezpośrednio dla słabości systemu
	niebezpośrednio przeznaczone do likwidacji słabości
	niemożliwe do zastosowania wobec słabości
	może zlikwidować ryzyko niebezpośrednio
	może zlikwidować ryzyko bezpośrednio

[25] *R. H. Anderson, Ph. M. Feldman, S. Gerwehr, B. K. Houghton, R. Mesic, J. Pinder, J. Rothenberg, J. R. Chiesa: Securing the U.S. Defense Information Infrastructure A Proposed Approach,*

CECHY SYSTEMU A PODATNOŚĆ NA ZAGROŻENIA

CECHY SYSTEMU / TECHNIKI OCHRONY PRZED ZAGROŻENIAMI		różnorodność	statyczna alokacja zasobów	dynamiczna alokacja zasobów	nadmiarowość	elastyczność / siła	szybkość odzysku i rekonstrukcji	oszukiwanie	segmentacja / decentralizacja / kwarantanna	identyfikacja odporności	samoorganizacja a zachowania zbiorowości	zarządzanie personelem	scentralizowane zarządzanie zasobami informacyjnymi	struktura ostrzegawcza przed zagrożeniami
właściwości architektury	unikalność			■		■	■			■	■			
	niezwykłość		■	■	■	■	■	■	■		■			
	centralizacja		■			■	■	■	■		■		■	
	rozłączność		■	■	■		■		■		■			
	jednorodność	■			■	■			■				■	
złożoność zachowań	wrażliwość	■		■		■	■	■	■	■	■			
	przewidywalność	■		■				■	■	■			■	
zdolność przystosowania i manipulacji	sztywność		■						■	■	■			
	elastyczność	■						■		■				
	naiwność			■						■				
działanie / konfiguracja	ograniczenia pojemności			■										
	brak możliwości odzysku		■	■		■		■		■				
	brak samoświadomości								■					
	trudności w zarządzaniu	■		■				■			■	■	■	
	samozadowolenie					■		■	■	■	■	■		■
niebezpośrednie / niefizyczne ujawnienie	dostępność elektroniczna		■	■				■	■	■				■
	przejrzystość							■						■
bezpośrednia / fizyczne ujawnienie	fizyczna dostępność		■	■	■	■	■	■	■					■
	wrażliwość elektromagn.	■	■		■	■	■	■	■					
obiekty tow. / infrastruktura	zależność	■		■	■	■			■		■		■	

Cechy systemu:

1. właściwości architektury, ta kategoria zawiera cechy, wynikające z architektury systemu:
   a. unikalność – unikalne rozwiązania są na ogół słabiej przetestowane i przez to mniej doskonałe;
   b. niezwykłość – jeżeli jakiś istotny komponent istnieje tylko w jednym miejscu to jego awaria może spowodować awarię systemu i spowodować, że stanie się on celem ataku;
   c. centralizacja – mówimy o systemie, że jest scentralizowany jeżeli decyzje, dane lub sterowanie muszą przechodzić (lub wychodzić) przez jeden węzeł lub proces;
   d. rozłączność – składniki lub procesy, które dają się łatwo wyizolować z systemu stają się potencjalnym celem ataku realizowanego zgodnie ze strategią „dziel i rządź";
   e. jednorodność (homogeniczność) – w przeciwieństwie do niezwykłości jednorodność określa wykorzystanie jednakowych rozwiązań co powoduje, że pojedynczy rodzaj ataku pozwala na uszkodzenie wielu elementów systemu;
2. złożoność zachowań, pokazujące, że część słabości systemu można łatwiej zidentyfikować poprzez jego zachowania niż strukturę lub implementację:
   a. wrażliwość – im bardziej wrażliwy jest system na zmiany we wprowadzaniu danych przez użytkownika lub niestandardowe formy użycia systemu tym łatwiejszym staje się celem ataku;
   b. przewidywalność – jest cechą zachowania się systemu, która rozpoznana przez napastnika pozwala mu wyciągać wnioski dotyczące zachowania się systemu po wykonaniu ataku
3. zdolność przystosowania i manipulacji – kategoria obejmująca takie cechy systemu, które określają łatwość zmian w systemie możliwych do realizacji wprost przez akcję użytkownika lub w odpowiedzi generowanej przez system na akcję. Chociaż elastyczność systemu jest na ogół jego zaletą to może również prowadzić do spowodowania jego podatności na zagrożenia:

a. sztywność – powodująca, że system jest trudniejszy do zaatakowania i złośliwej modyfikacji ale po pokonaniu jest trudniejszy do takiego zmodyfikowania, żeby zwiększyć jego odporność;
b. elastyczność – przeciwieństwo sztywności;
c. naiwność – nieodporny na proste i oczywiste zachowania, np. brak kontroli wejść;

4. działanie / konfiguracja – słabe punkty systemu w tej kategorii wynikają ze sposobów w jaki system lub procesy są: konfigurowane, zarządzane, wykonywane lub administrowane:
   a. ograniczenia pojemności – dla systemu pracującego w pobliżu granic swoich możliwości istnieje duża łatwość przekroczenia tych granic i uniemożliwienia jego działania;
   b. brak możliwości odzysku – ponieważ praktycznie każdy system ma możliwość odzysku (w szczególnym przypadku odbudowanie) utraconych zasobów, ta cecha będzie oznaczała konieczność poświęcenia zbyt dużego czasu i wysiłku na odzysk;
   c. brak samoświadomości – brak możliwości śledzenia przez system własnego działania prowadzi do niemożliwości wykrycia ataków na niego przeprowadzanych;
   d. trudności w zarządzaniu – trudności związane z właściwą konfiguracją systemu wynikające z jego złożoności powodują, że nawet uświadomione słabości systemu nie są eliminowane;
   e. samozadowolenie – wynikające z rutynowego podchodzenia do spraw współpracy człowieka z systemem powodują powstanie wielu problemów związanych z bezpieczeństwem systemu;
5. niebezpośrednie / niefizyczna ujawnienie - obejmujące słabości systemu wynikające z łatwości zdalnego dostępu lub łatwości dostępu do wiadomości o nim:
   a. dostępność elektroniczna – możliwość bezpośredniego dostępu do systemu bez konieczności realizowania jakichkolwiek dodatkowych operacji;
   b. przejrzystość – polegające na upublicznieniu informacji na temat systemu poprzez np. podaniu do ogólnej wiadomości kodu źródłowego oprogramowania;

6. bezpośrednie / fizyczne ujawnienie – takie słabości systemu, które dają możliwości bezpośredniego, fizycznego ataku:
   a. fizyczna dostępność, określająca łatwość fizycznego dostępu do elementów systemu takich jak: linie telekomunikacyjne, urządzenia peryferyjne, zasilanie energetyczne itp.;
   b. wrażliwość elektromagnetyczna, określająca możliwość dostępu bezpośredniego do energii emitowanej przez urządzenia systemu co pozwala na zakłócanie, kradzież bądź zniszczenie elementów systemu;
7. Obiekty towarzyszące / infrastruktura – zależność systemów informatycznych od obiektów towarzyszących powoduje zwiększenie możliwości zaistnienia słabych punktów tych systemów

Techniki ochrony przed zagrożeniami:

1. Różnorodność (heterogeniczność) – to obecność w systemie różnorodnych rozwiązań powodująca utrudnienia w przeprowadzeniu ataku i wymagająca stosowania różnych technik ataku. Możliwe jest stosowanie różnorodności przestrzennej, rozmieszczając różne rozwiązania realizujące te same funkcje w różnych miejscach systemu np. korzystanie z usług różnych dostawców usług telekomunikacyjnych; albo czasowa, łatwiejsza do zrealizowania w warstwie oprogramowania systemu polegająca na zmianie alokacji elementów systemu w trakcie jego działania, np. miejsce składowania elementów bazy danych, procedur itp.
2. Statyczna alokacja zasobów – umieszczanie krytycznych zasobów systemu, zarówno sprzętu jak i oprogramowania, w specjalnych, szczególnie dobrze zabezpieczonych obszarach.
3. Dynamiczna alokacja resursów – polegająca na alokacji istotnych elementów systemu w zależności od ich ważności w różnych miejscach. System zmienia miejsca alokacji w zależności od zmian zachodzących w jego środowisku co wymaga również umiejętności nadawania priorytetów dynamicznie alokowanym zasobom w zależności od podejmowanych działań.
4. Nadmiarowość (redundancja) – zwielokrotnianie niektórych elementów systemu lub duplikowanie kluczowych informacji powoduje, że ich utrata w wyniku wystąpienia zagrożenia nie jest groźne dla systemu.
5. Elastyczność / siła – to te techniki, które powodują, że pojedyncze elementy systemu są w stanie samodzielnie udaremnić lub zaabsorbować atak bez

konsekwencji dla systemu jako całości. Są to techniki związane z użyciem firewalli i technik kryptograficznych.

6. Szybkość odzysku i rekonstrukcji – to technika pozwalająca na odzyskanie utraconych elementów systemu w ciągu dopuszczalnie długiego czasu.
7. Oszukiwanie – to wykorzystanie takiej techniki zabezpieczeń, która powoduje, że przeciwnik zachowuje się w sposób zgodny z naszym życzeniem ze względu na to, iż odczytał właściwości naszego systemu tak jak mu to zasugerowano i wprowadzono w błąd.
8. Segmentacja, decentralizacja i kwarantanna – te techniki stosuje się w celu odizolowania lokalnych uszkodzeń, aby nie dopuścić do rozszerzania się zniszczeń. Segmentacja to taki sposób kreowania i konfigurowania systemu, aby jego elementy mogły działać autonomicznie. Decentralizacja wykorzystuje metodę rozproszenia najważniejszych punktów węzłowych systemu aby zmniejszyć szansę unicestwienia systemu poprzez pokonanie jednego punktu. Kwarantanna natomiast powoduje odizolowanie zaatakowanej części systemu w celu zapobieżenia rozprzestrzenianiu się zniszczeń bądź możliwości wniknięcia do pozostałej części systemu.
9. Identyfikacja odpornościowa – technika będąca w fazie wprowadzania, niecałkowicie zaimplementowana opierająca się na analogiach do biologicznego systemu immunologicznego. Stosuje się tu takie metody jak: wyodrębnienie „dziwnych" zachowań w systemie, zapamiętywanie działań wrogich i efektywności zastosowanych sposobów reakcji w celu zastosowania adekwatnych środków w przyszłości, ciągła i wszechobecna ochrona polegająca na ciągłym sprawdzaniu użytkowników systemu bez względu na stopień zaufania do nich.
10. Samoorganizacja i zachowania zbiorowe – to techniki, u których podstawy legły obserwacje takich systemów przyrodniczych jak ule czy mrowiska, a w których można zauważyć takie cechy przydatne również w organizacji ochrony systemów informacyjnych jak: zachowania zorientowane na osiągnięcie celu czy specjalizacja. Pierwsza z tych cech znajduje swoje odbicie w wykorzystywaniu do tworzenia sieci procesów adaptacyjnych czy sieci neuronowych, które nie potrzebują centralnego sterowania aby przystosować się do zaistniałych warunków. Druga natomiast polega na takiej samoorganizacji systemu, aby niektóre jego elementy mogły spełniać tylko zadania ochronne inne zaś wykonywać inne specjalizowane zadania.

11. Zarządzanie personelem – w celu wyeliminowania zagrożeń wynikających z działań ludzi zatrudnionych przy systemie należy uświadamiać im istnienie zagrożeń, szkolić i kształcić, monitorować ich zachowania oraz karać za przekroczenia procedur bezpieczeństwa.
12. Scentralizowane zarządzanie zasobami informacyjnymi – trzy z powyższych technik: heterogeniczność, dynamiczna alokacja zasobów i redundancja wymagają dostępności alternatywnych systemów bądź ich elementów dlatego określenie, który z nich ma być wykorzystywany musi być realizowane metodą centralnego zarządzania zasobami.
13. Struktura ostrzegawcza przed zagrożeniami – powinna istnieć specyfikacja poziomów zagrożenia i związanych z nim akcji, które należy podejmować w celu przeciwdziałania.

Każda z cech systemu i każda z technik pozwalających na zminimalizowanie słabości systemów informacyjnych może mieć różną implementację w zależności od stopnia jego złożoności organizacyjnej i technologicznej. Powoduje to, że proces modelowania tych zagadnień będzie wymagał dużego wysiłku związanego z dokładnym rozpoznaniem analizowanego systemu i ryzyka wystąpienia określonych zagrożeń.

Badania nad możliwością reakcji systemu na wystąpienie określonych zagrożeń muszą być prowadzone w warunkach dużej nieokreśloności. Wiadomo, że najsłabszym ogniwem w systemie ochrony informacji jest człowiek a nie środki, którymi się posługuje, dlatego też szkolenie i treningi osób odpowiadających bezpośrednio lub pośrednio za system jest jednym z podstawowych sposobów przeciwdziałania zagrożeniom. Gry decyzyjne (kierownicze) są z pewnością jednym z najefektywniejszych sposobów doskonalenia takich umiejętności, które pozwolą na podejmowanie właściwych decyzji w przypadku zaistnienia sytuacji kryzysowej.

Mimo wyraźnej specyfiki działań prowadzonych wobec systemów informacyjnych wojsk nieprzyjaciela trzeba powiedzieć, że w wielu aspektach będą one zbieżne lub nawet tożsame z działalnością wobec systemów informacyjnych państwa (Infrastruktury Krytycznej Państwa), a ponieważ sfera bezpieczeństwa państwa jest nierozerwalnie związana ze sferą militarną dlatego modelowanie walki informacyjnej musi obejmować obydwa wymienione wyżej obszary.

Powyższe uwagi pozwalają stwierdzić, że analizując wpływ bezpieczeństwa informacyjnego na bezpieczeństwo państwa w kontekście walki informacyjnej należy

wyraźnie rozgraniczyć w czasie sprawy związane z ochroną Infrastruktury Krytycznej Państwa, która jest działaniem ciągłym, od militarnych operacji informacyjnymi, które realizowane są przeważnie w kolejnych fazach narastającego kryzysu międzynarodowego, aczkolwiek jedne i drugie mają swoje źródło w rozwoju technologii teleinformatycznych. Realizując zatem badania symulacyjne nad tymi zagrożeniami i przeciwdziałaniem im trzeba uwzględniać bardzo wiele uwarunkowań, które pozwolą w sposób jednoznaczny określić czy skutki wystąpienia zagrożeń pozwalają na stwierdzenie czy mamy do czynienia z działaniami wojennymi, terrorystycznymi, przestępstwami komputerowymi czy też niewybrednymi dowcipami. Ta kwalifikacja pozwala na podjęcie działań adekwatnych do zaistniałej sytuacji. Cienka granica pomiędzy wszystkimi wymienionym wyżej działaniami wymusza dużą ostrożność w podejmowanych środkach retorsyjnych. Zastosowanie gwałtownych i o dużym nasileniu działań odwetowych podjętych ze względu na ryzyko poniesienia dużych strat niesie jednocześnie za sobą ryzyko wywołania głębokiego konfliktu międzynarodowego a przy okazji trudne do określenia skutki dla rozwoju form „życia" w cyberprzestrzeni.

Symulacja działań wojny informacyjnej sprowadzać się zatem będzie do sprawdzenia odporności systemów informacyjnych na zagrożenia. Prowadzone w tej chwili audyty bezpieczeństwa informacyjnego, wykorzystanie skanerów bezpieczeństwa[26], systemów wykrywania włamań[27] czy testów penetracyjnych[28] dają odpowiedź na pytania o bezpieczeństwie informacji, a więc również organizacji, instytucji czy państw. Wnioski, które można wyciągnąć z takich badań dają podstawy do przeprowadzenia zmian, które pozwolą na podwyższenie stanu bezpieczeństwa informacyjnego. Wyjątkowa złożoność systemu Infrastruktury Krytycznej Państwa, przejawiająca się również w różnorodności zastosowanych rozwiązań technicznych jest jeszcze jednym powodem, dla którego badanie symulacyjne efektów wojny informacyjnej jest wyjątkowo trudne, tym niemniej zwłaszcza sfera organizacyjna wymaga ciągłego doskonalenia wraz z wyjątkowo szybkim rozwojem metod zagrażania systemom.

---

[26] *systemy wykrywające słabe punkty badanych systemów i sieci teleinformatycznych*

[27] *Systemy wykrywania włamań (ang. intrusion detection system) wykrywa nadużycia i anomalie, umożliwia wykrywanie, alarmowanie i blokowanie ataków z sieci oraz niedozwolonych działań użytkowników lokalnych*

[28] *„Istotą testów penetracyjnych jest jak najbliższe naśladowanie działań hakerów. Można powiedzieć że są to autoryzowane przez klienta próby włamania do sieci. Przy zamawianiu tego typu testu trzeba ustalić jak wiele informacji o infrastrukturze sieciowej będzie posiadał wykonujący test. Należy pamiętać że testy zmierzają do oceny stopnia bezpieczeństwa sieci. Ocena ta jest ściśle związana z przyjętymi założeniami, a najważniejszym założeniem powinna być ilość informacji, którą na wstępie posiada potencjalny intruz." za Wojciech Dworakowski „Testowanie bezpieczeństwa - metody, narzędzia, błędy..."*

Bibliografia:

1. R. H. Anderson, Ph. M. Feldman, S. Gerwehr, B. K. Houghton, R. Mesic, J. Pinder, J. Rothenberg, J. R. Chiesa: "Securing the U.S. Defense Information Infrastructure A Proposed Approach",
2. J. Arquilla, D. Ronfeld: "Cyberwar is Coming", artykuł dla RAND Corporation
3. K. Ćwiklik: „Analiza systemowa zjawiska wojny informacyjnej", AON Warszawa, 2003
4. M. G. Devost: "Political Aspects of Class III Information Warfare: Global Conflict and Terrorism", InfoWarCon II, Montreal 1995
5. R. Gogela, L. Novàk, A. Šefčik: "Critical Infrastructure Modelling", w Security and Protection of Information 2003,
6. L. T. Greenberg, S. E. Goodman, K. J. Soo Hoo: "Information Warfare and International Law", National Defense University Press,
7. R. R. Fogelman: "Cornerstones of Information Warfare"
8. R. R. Fogelman: "Information Operations: The Fifth Dimension of Warfare" w mowie wygłoszonej do Stowarzyszenia Łączności i Elektroniki Sił Zbrojnych USA, 25.04.1995,
9. B. C. Lewis: "Information Warfare"
10. M. Libicki: "What is Information Warfare?", artykuł dla Institute for National Strategic Studies
11. "The National Strategy to Secure Cyberspace", Washington DC, 2003
12. G. Nowacki:"Współczesne poglądy na prowadzenie walki informacyjnej", AON, Warszawa 2001
13. „Regulamin działań wojsk lądowych", Warszawa, 1999
14. „Rozpoznanie wojskowe", Szt. Gen. WP 1531/2001