*Symulacja w Badaniach i Rozwoju*
Vol. 9, No. 1-2/2018

**Romuald HOFFMANN**
Wojskowa Akademia Techniczna,
Wydział Cybernetyki, Instytut Systemów Informatycznych
ul. gen. Witolda Urbanowicza 2, 00-908 Warszawa 46
E-mail: romuald.hoffmann@wat.edu.pl

# Modelowanie w języku dynamiki systemowej operacji cybernetycznych z wykorzystaniem modeli walki łączonych z modelami rozprzestrzeniania się kodu złośliwego

## 1 Wprowadzenie

Metoda dynamiki systemowej (ang. *system dynamics*) jest metodą budowy modeli symulacji ciągłej, która umożliwia modelowanie struktury oraz dynamiki złożonych systemów i procesów w nich zachodzących. Została zaproponowana w latach 60. XX wieku przez Jaya Forrestera, który opracował jej podstawowe zasady i przedstawił je w licznych publikacjach, np. [6], [7], [8] (Forester 1961, 1969, 1975). Metoda dynamiki systemowej jest przeznaczona do modelowania złożonych systemów, w których występują sprzężenia zwrotne opisujące zależności przyczynowo-skutkowe pomiędzy elementami systemu [9] (Hoffmann, Protasowicki 2013). W modelach matematycznych zbudowanych z wykorzystaniem metody dynamiki systemowej wyróżniamy równania: poziomów (opisane równaniami różniczkowymi pierwszego rzędu), przepływów (dane równaniami algebraicznymi) i zmiennych pomocniczych (określone jako równania algebraiczne). Z równań tych otrzymujemy układ równań różniczkowo-algebraicznych, stanowiący opis matematyczny związków przyczynowo-skutkowych występujących w modelowanym systemie. W metodzie dynamiki systemowej stosowane są równania różniczkowe zwyczajne pierwszego rzędu wyprowadzone z ogólnej postaci zagadnienia Cauchy'ego [12] (Kasperska 2005). Bardzo dobrym wprowadzeniem do dynamiki systemowej jest praca Stermana [28]. Przykłady zastosowania dynamiki systemowej do modelowania procesów walki w oparciu o podejście Lanchestera zostały przedstawione w pracy [10] (Hoffmann, Protasowicki 2013).

Lanchester (1916) [19], [20] analizując dynamikę walk powietrznych podczas I wojny światowej, zastosował do modelowania ilościowego procesu walki dwóch przeciwników parę liniowych zwyczajnych równań różniczkowych. Od tamtego czasu model Lanchestera był inspiracją dla wielu badaczy, którzy przyczynili się do szeregu publikacji, a których nie sposób wyczerpująco wymienić w tym miejscu. Warto jednak zwrócić uwagę na prace: [24] (Morse, Kimball 1951), [3], [4] (Bracken i inni 1995), [30] (Washburn, Kress 2009), [17] (Kress 2012), [29] (Tolk 2012). Prawie całość dostępnych publikacji dotyczy modeli dynamiki walki dwóch stron. Ciekawsze modele, jakimi są modele walki trzech lub więcej stron, można odnaleźć tylko w nielicznych pracach – najnowsze to: [21] (Lin, MacKay 2014), [18] (Kress i inni 2018).

Murray (1988) [25] jako pierwszy zasugerował związek pomiędzy epidemiologią a wirusami komputerowymi, zauważając, że wirusy komputerowe są pewną analogią wirusa biologicznego. Kephart i White (1991, 1993) [14], [15] byli pierwszymi autorami, którzy zaproponowali przyjęcie modelu SIS (ang. *susceptible, infected, susceptible*) jako modelu rozprzestrzeniania się wirusów komputerowych. Od tego czasu modele epidemiologiczne są szeroko stosowane do modelowania dynamiki rozprzestrzenia się wirusów komputerowych. Modele epidemii (rozprzestrzeniania się) kodu złośliwego można podzielić na dwie kategorie – modele deterministyczne, oparte na równaniach różniczkowych, i modele stochastyczne, wykorzystujące w większości przypadków łańcuchy Markowa, procesy gałązkowe i procesy dyfuzji. W niniejszej pracy bazujemy na deterministycznych modelach epidemii. Porównanie deterministycznych oraz stochastycznych modeli SIS i SIR (ang. *susceptible, infected, recovered*) można znaleźć w wybranych publikacjach: [1] (Allen, Burgin 2000), [2] (Allen 2008), [13] (Keeling, Ross 2008), [5] (Britton 2010). Należy tutaj zaznaczyć, że zarówno deterministyczne, jak i stochastyczne modele odgrywają znaczącą rolę w modelowaniu dynamiki zjawisk epidemii. Wskazuje na to istniejąca bogata literatura, w większości dotycząca deterministycznych modeli epidemiologicznych rozprzestrzeniania się wirusów komputerowych. Oprócz klasycznych modeli SIS i SIR, bazujących na modelu Kermacka i McKendricka (1927) [16], w ostatnich latach zostało sformułowanych wiele nowych. Hoffmann i Protasowicki (2007) [11] przedstawili w ujęciu dynamiki systemowej deterministyczne modele podstawowe SIS, SIR, SIRS, a także model SAI (ang. *susceptible, antidotal, infected*) jako uproszczoną wersję modelu SIRA (ang. *susceptible, infected, removed, antidotal*) opracowanego przez Piqueira i Araujo (2009) [26].

Niezaprzeczalnie współczesny rozwój technologii informatycznych umożliwił prowadzenie operacji militarnych również w cyberprzestrzeni. W tej sytuacji oprogramowanie złośliwe stało się bronią umożliwiającą prowadzenie operacji cybernetycznych, samodzielnych lub wspierających działania kinetyczne[1]. Same modele epidemiologiczne do modelowania skutków operacji cybernetycznych wydają się już niewystarczające. Stąd obiecującym kierunkiem badań nad modelami dynamiki walki z wykorzystaniem kodu złośliwego wydaje się połączenie podejścia Lanchestera i modeli epidemiologicznych. Tutaj warto zwrócić uwagę na pracę[2] Schramma i Gavera (2013) [27], którzy modelując prowadzenie operacji cybernetycznej poprzez propagację kodu złośliwego (np. wirusów, robaków) w systemach przeciwnika w połączeniu z działaniami kinetycznymi, przedstawili podejście połączenia klasycznego modelu walki bezpośredniej Lanchestera (ang. *aimed fire*) z modelem rozprzestrzeniania się kodu złośliwego SIR (ang. *susceptible, infected, removed*).

W tym kontekście model SAI w ujęciu dynamiki systemowej [11] (Hoffmann, Protasowicki 2017) zostanie wykorzystany w niniejszej pracy i w połączeniu z klasycznym modelem Lanchestera stanowić będzie przedmiot dalszych rozważań.

[1] tzn. operacje militarne, z którymi bezpośrednio wiążą się straty ludzi i/lub uzbrojenia
[2] jak do tej pory jedyną

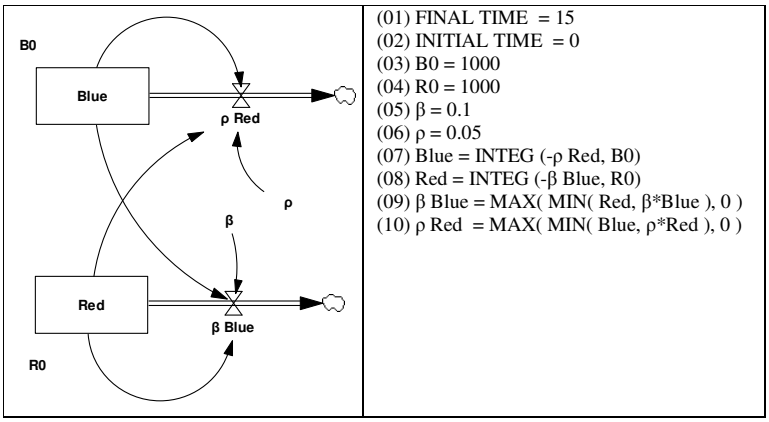
## 2 Klasyczne modele walki Lanchestera w ujęciu dynamiki systemowej

W pracy podstawą modelowania matematycznego dynamiki walki są modele W.F. Lanchestera ujęte w konwencji klasycznej dynamiki systemowej. Przypomnę, że liczne modele ogólnie zwane modelami Lanchestera obejmują w większości rodzinę modeli matematycznych wykorzystujących równania różniczkowe, zarówno liniowe, jak i nieliniowe. Właśnie ta własność umożliwia proste przedstawienie modeli dynamiki walki w języku klasycznej dynamiki systemowej. Generalnie model Lanchestera opisującego dynamikę walki dwóch stron Blue i Red można przedstawić następująco:

$$\begin{aligned} \frac{dB(t)}{dt} &= -\rho_R(t)\,, \\ \frac{dR(t)}{dt} &= -\beta_B(t) \end{aligned} \tag{1}$$

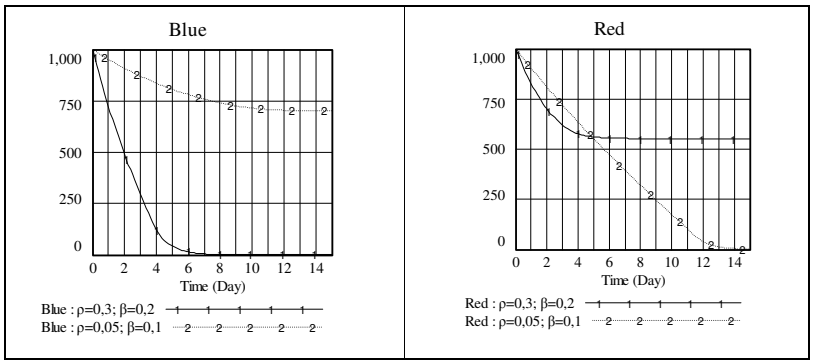
z warunkami początkowymi: $B(0) = B_0 > 0$, $R(0) = R_0 > 0$, gdzie funkcje $B(t), R(t)$ opisują stan liczebny stron walczących w chwili $t \geq 0$ odpowiednio: Blue, Red, natomiast $\rho_R(t), \beta_B(t)$ są funkcjami opisującymi intensywność zadawania strat stronom przeciwnym. W modelowaniu walki układ (1) jest sensowny dla takiego przedziału czasu $[0, T]$, że dla każdego $t \in [0, T]$ funkcje $B(t) > 0$ i $R(t) > 0$.

Przykładowy matematyczny model walki bezpośredniej Lanchestera w języku dynamiki systemowej opisany układem równań (1) przedstawia rysunek 1. Natomiast wyniki przykładowej symulacji przedstawia na rysunek 2. W przykładzie przyjęto, że $\rho_R(t) = \rho \cdot R(t)$ oraz $\beta_B(t) = \beta \cdot B(t)$, gdzie współczynniki $\rho, \beta$ są stałe.




*Rys. 1. Przykładowy model Lanchestera opisany układem równań (1) w ujęciu dynamiki systemowej*

*Fig. 1. An example of the Lanchester combat model described by the system of equations (1) in terms of system dynamics*




*Rys. 2. Przykładowe wyniki symulacji modelu Lanchestera z rysunku 1*

*Fig. 2. Sample results of simulation of Lanchester combat model from Figure 1*

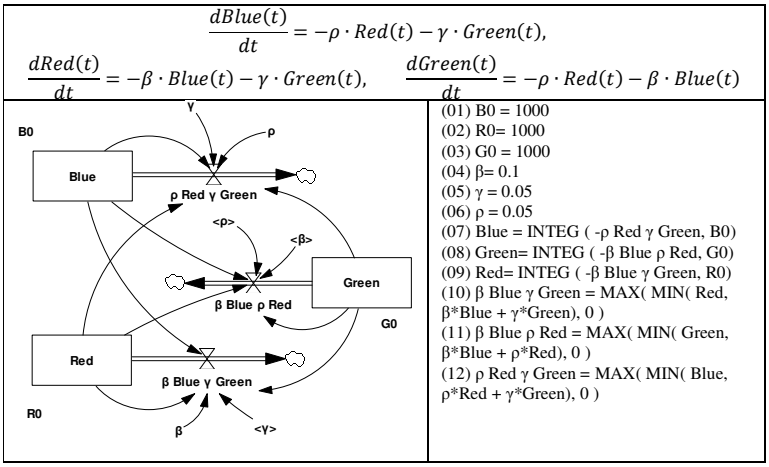
W tym miejscu również warto sformułować w konwencji dynamiki systemowej model opisującego dynamikę walki trzech wzajemnie wrogich stron: Blue, Red i Green.

Zakładając dla uproszczenia, że każda ze stron niszczy zasoby przeciwników z taką samą skutecznością, model matematyczny Lanchestera przyjmuje postać:

$$\begin{aligned} \frac{dB(t)}{dt} &= -\rho_R(t) - \gamma_G(t)\,, \\ \frac{dR(t)}{dt} &= -\beta_B(t) - \gamma_G(t)\,, \\ \frac{dG(t)}{dt} &= -\rho_R(t) - \beta_B(t) \end{aligned} \tag{2}$$

z warunkami początkowymi: $B(0) = B_0 > 0$ , $R(0) = R_0 > 0$ , gdzie funkcje $B(t), R(t), G(t)$ opisują stan liczebny stron walczących w chwili $t \geq 0$ odpowiednio: Blue, Red, Green, natomiast $\beta_B(t), \rho_R(t), \gamma_G(t)$ są funkcjami opisującymi intensywność zadawania strat stronom przeciwnym. Układ równań (2) ma sens w modelowaniu walki, gdy dla każdego $t \in [0, T]$ funkcje $B(t) > 0$ i $R(t) > 0$.

Przykładowy matematyczny model Lanchestera walki bezpośredniej trzech stron w języku dynamiki systemowej opisany układem równań (2) przedstawia rysunek 3. W przykładzie przyjęto, że $\beta_B(t) = \beta \cdot B(t)$, $\rho_R(t) = \rho \cdot R(t)$ oraz $\gamma_G(t) = \gamma \cdot G(t)$, gdzie współczynniki $\beta, \rho, \gamma$ są stałe.




*Rys. 3. Przykładowy model Lanchestera dla trzech stron w ujęciu dynamiki systemowej*

*Fig. 3. An example of the Lanchester model for three-way combat in terms of system dynamics*

## 3 Model SAI rozprzestrzeniania się kodu złośliwego

Rozważę model SAI (ang. susceptible, antidotal, infected), który w konwencji dynamiki systemowej [10] (Hoffmann, Protasowicki 2013) zostanie wykorzystany w dalszej części pracy w połączeniu z klasycznym modelem dynamiki walki bezpośredniej Lanchestera. W modelu przyjęto założenie, że rozprzestrzenianie się kodu złośliwego prowadzi do podziału populacji komputerów na trzy grupy urządzeń:

- podatne $(S(t), \mathrm{t} \geq 0)$ – takie, które mogą zostać zainfekowane,
- zainfekowane $(I(t), \mathrm{t} \geq 0)$ oraz
- uodpornione $(A(t), \mathrm{t} \geq 0)$ w wyniku usunięcia podatności i aktualizacji oprogramowania.

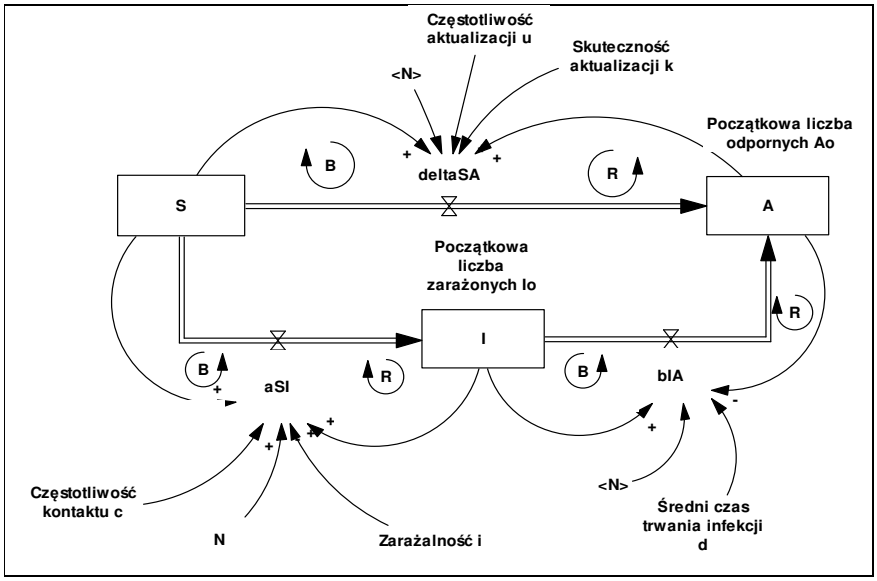
Model SAI jest opisany następującym układem równań różniczkowych [26] (Piqueira, Araujo 2008):

$$\begin{aligned} \frac{d}{\mathrm{dt}} S(t) &= -a \cdot S(t) \cdot I(t) - \delta \cdot S(t) \cdot A(t), \\ \frac{d}{dt} I(t) &= a \cdot S(t) \cdot I(t) - b \cdot I(t) \cdot A(t), \\ \frac{d}{dt} A(t) &= \delta \cdot S(t) \cdot A(t) + b \cdot I(t) \cdot A(t) \end{aligned} \tag{3}$$

z wymaganymi warunkami początkowymi: $S(0) = S_0 > 0$, $I(0) = I_0 > 1$, $A(0) = A_0 > 0$. Parametr $a > 0$ oznacza współczynnik (tempo) rozprzestrzeniania się wirusa komputerowego, $b > 0$ jest współczynnikiem (tempem) usuwania kodu złośliwego, natomiast parametr $\delta > 0$ oznacza współczynnik skuteczności usunięcia podatności lub aktualizacji oprogramowania. Założenie stałej wielkości populacji

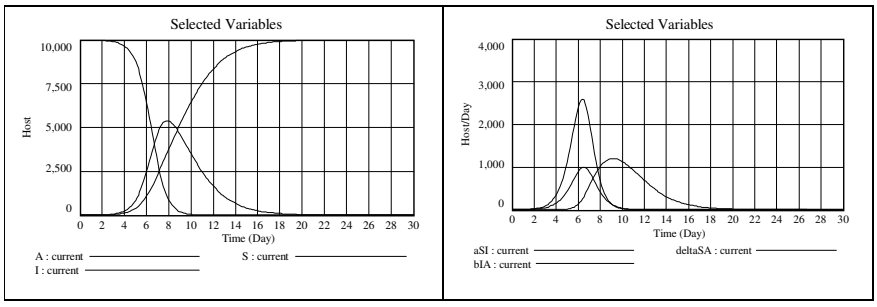
komputerów jest już wbudowane w układ równań (3), tzn. $S(t) + I(t) + A(t) = \text{const} = N$.

Model SAI w ujęciu dynamiki systemowej [11] (Hoffmann, Protasowicki 2017) przedstawia rysunek 4. W modelu tym przyjęto $a = c \cdot i/N > 0$, $b = 1/d > 0$, $\delta = u \cdot k/N$ . Wyniki przykładowej symulacji modelu SAI zostały przedstawione na rysunku 5.




*Rys. 4. Model SAI opisany układem równań (3) w ujęciu dynamiki systemowej*

*Fig. 4. The SAI model described by the system of equations (3) in terms of system dynamics*




*Rys. 5. Przykładowe wyniki symulacji modelu SAI z rys. 4 (liczba komputerów N = 10 000; czas symulacji 30; c = 6; d = 2; i = 0,25; u = 2; k = 0,65; $I_0$ = 1; $A_0$ = 1)*

*Fig. 5. Sample results of the simulation of SAI model from Fig. 4. (number of computers N = 10 000; simulation time 30; c = 6; d = 2; i = 0,25; u = 2; k = 0,65; $I_0$ = 1; $A_0$ = 1*

## 4 Model dynamiki walki z użyciem kodu złośliwego przez stronę Red

Przytoczę dalej model Schramma i Gavera (2013) [27], którzy modelując prowadzenie operacji kinetycznych w połączeniu z operacją cybernetyczną poprzez propagację[3] kodu złośliwego w systemach przeciwnika, wykorzystali model walki bezpośredniej Lanchestera oraz zmodyfikowany model SIR. Założono, że siły stron wykorzystują systemy komputerowe w walce i eliminacja kinetyczna członka strony przeciwnej eliminuje z walki również wyposażenie komputerowe. Dodatkowo przyjęto założenie, że strona Red – w przeciwieństwie do strony Blue – jest niepodatna na ataki komputerowe oraz wprowadziła kod złośliwy do systemów przeciwnika. Chociaż założenie to wydawać się może nierealne, to jednak odpowiada na przykład przypadkowi, kiedy strona Red posiada systemy wykonane w odmiennej technologii, niepodatnej na ataki cybernetyczne, i posiada zdolność wcześniejszego wprowadzenia kodu złośliwego do systemów tegoż przeciwnika.

W tym miejscu warto zauważyć, że zmodyfikowany model SIR użyty przez Schramma i Gavera [27] jest w swej istocie modelem różniącym się od modelu SAI założeniem, że intensywność aktualizacji komputerów podatnych różni się od intensywności usuwania kodu złośliwego (połączonego z aktualizacją). Zatem na potrzeby artykułu zostanie przyjęty model SAI i w konsekwencji używane będą oznaczenia z modelu SAI dotyczące funkcji opisujących liczbę w czasie komputerów podatnych $S(t)$, zainfekowanych $I(t)$ i uodpornionych $A(t)$. Liczebność stron w czasie $t \geq 0$ opisują funkcje $R(t)$, $B(t) = S(t) + I(t) + A(t)$ odpowiednio stron: Red, Blue. Zatem pierwotny model Schramma i Gavera [27] z wymaganymi warunkami początkowymi: $(0) = R_0 > 0$, $S(0) = S_0 > 0$, $I(0) = I_0 > 0$ , $A(0) = A_0 > 0$ można przedstawić następującym układem równań różniczkowych:

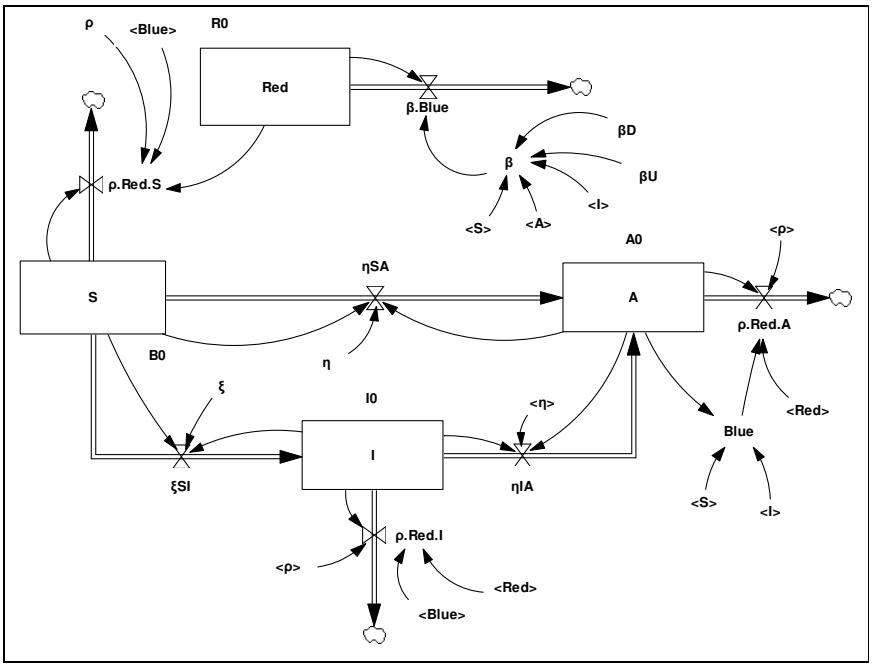
$$\begin{aligned}
\frac{d}{dt} R(t) &= -\beta_U \cdot \big(\mathrm{S}(t) + A(t)\big) - \beta_I \cdot I(t)\,, \\
\frac{d}{\mathrm{dt}} S(t) &= -\xi \cdot S(t) \cdot I(t) - \eta \cdot S(t) \cdot A(t) - \rho \cdot R(t) \cdot \frac{S(t)}{B(t)}\,, \\
\frac{d}{dt} I(t) &= \xi \cdot S(t) \cdot I(t) - \eta \cdot I(t) \cdot A(t) - \rho \cdot R(t) \cdot \frac{I(t)}{B(t)}\,, \\
\frac{d}{dt} A(t) &= \eta \cdot S(t) \cdot A(t) + \eta \cdot I(t) \cdot A(t) - \rho \cdot R(t) \cdot \frac{A(t)}{B(t)}\,, \\
B(t) &= S(t) + I(t) + A(t)\,.
\end{aligned} \tag{4}$$

Parametr $\xi > 0$ oznacza współczynnik (tempo) rozprzestrzeniania się wirusa komputerowego; $\eta > 0$ jest współczynnikiem (tempem) zarówno usunięcia podatności (aktualizacji) oprogramowania, jak i usuwania kodu złośliwego; $\rho > 0$ oznacza współczynnik skuteczności (efektywność) rażenia kinetycznego sił Blue przez stronę Red. Natomiast współczynniki $\beta_U$, $\beta_I$ $(\beta_U > \beta_I)$ oznaczają skuteczności (efektywności) rażenia kinetycznego sił Red przez stronę Blue, gdzie $\beta_U$ dotyczy wykorzystania do walki kinetycznej systemów komputerowych zarówno podatnych

[3] wcześniej wprowadzonego

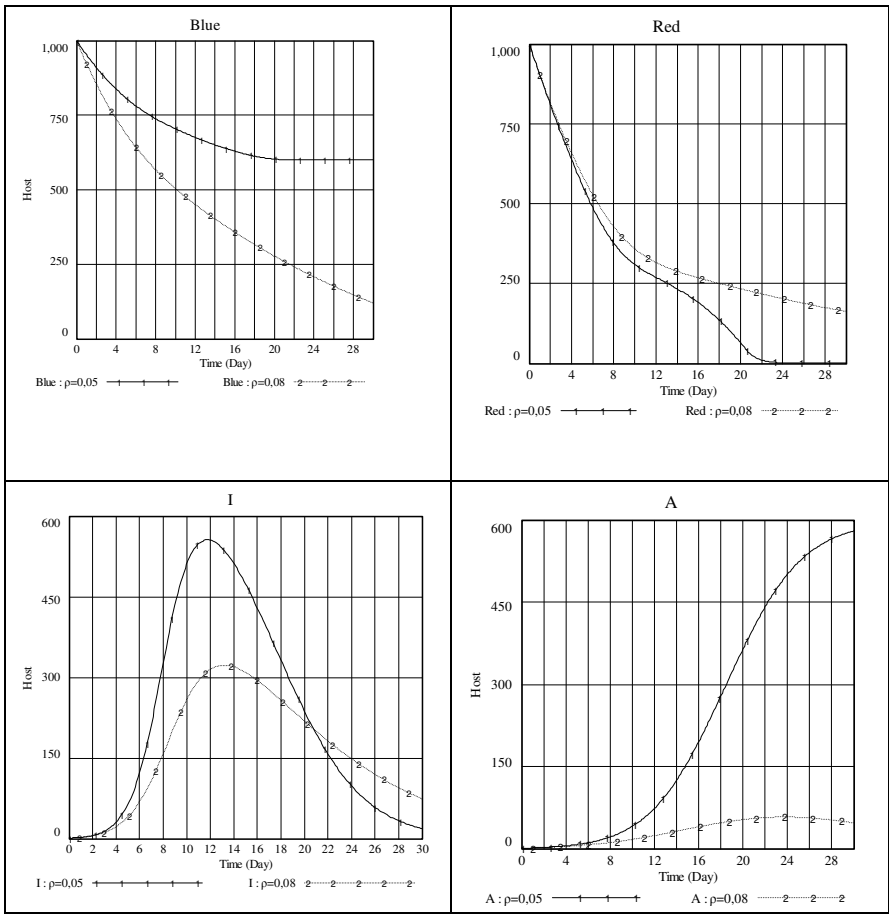
i odpornych, $\beta_I$ – zainfekowanych. Wartości współczynników $\rho,\ \eta,\ \xi,\ \beta_I,\ \beta_U$ są stałe. Układ (4) jest słuszny dla takiego przedziału czasu $[0,T]$, że dla każdego $t \in [0,T]$ funkcje $R(t) > 0$, $\mathrm{S}(t) > 0$, $I(t) > 0$ oraz $A(t) > 0$ .

Przykładowy model w języku dynamiki systemowej opisany układem równań (4) przedstawia rysunek 6, a wyniki przykładowej symulacji zostały podane na rysunku 7.




*Rys. 6. Przykładowy model walki Schramma i Gavera opisany układem równań (4) w ujęciu dynamiki systemowej*

*Fig. 6. An example of Schramm & Gaver's combat model described by the system of equations (4) in terms of system dynamics*




*Rys. 7. Przykładowe wyniki symulacji modelu dynamiki z rys. 6*

*Fig. 7. Sample results of simulation of the combat model from Fig. 6*

## 5 Model dynamiki walki z użyciem kodu złośliwego przez obie strony

Rozpatrzę wcześniej przytoczony model Schramma i Gavera [27], przy dodatkowym założeniu, że strona Red posiada systemy podatne na atak kodem złośliwym. Oznacza to, że w tym przypadku każda ze stron jest podatna na atak cybernetyczny. Oczywiście, utrzymam założenie wcześniejszej infekcji systemów, w tym przypadku obu stron. Ponadto przyjmuję założenie, że siły przeciwnych stron wykorzystują systemy komputerowe w walce i eliminacja kinetyczna członka strony przeciwnej eliminuje z walki również wyposażenie komputerowe.

Przed zdefiniowaniem układu równań różniczkowych przyjmuję następującą konwencję oznaczeń. Indeksem $i = 1,2$ oznaczać będzie się parametry modelu odpowiadające

stronom konfliktu, odpowiednio Blue przez $i = 1$ oraz Red przez $i = 2$. Dla $i = 1,2$ parametry $\xi_i > 0$, oznaczają współczynniki tempa rozprzestrzeniania się wirusa komputerowego; $\eta_i > 0$ są współczynnikami tempa zarówno usunięcia podatności (aktualizacji) oprogramowania, jak i usuwania kodu złośliwego; $\rho_i > 0$ oznaczają współczynniki skuteczności (efektywność) wzajemnego rażenia kinetycznego sił odpowiednio Blue przez stronę Red, Red przez Blue, Natomiast współczynniki $\beta_U$, $\beta_I$ ($\beta_U > \beta_I$) oznaczają skuteczności (efektywności) rażenia kinetycznego sił Red przez stronę Blue, gdzie $\beta_U$ dotyczy wykorzystania do walki kinetycznej systemów komputerowych zarówno podatnych, jak i odpornych, $\beta_I$ – zainfekowanych. Natomiast współczynniki $\rho_U$, $\rho_I$ ($\rho_U > \rho_I$) odpowiednio odnoszą się do skuteczności rażenia kinetycznego sił Blue przez stronę Red. Ponadto przyjmuję dla strony Blue ($i = 1$) oraz Red ($i = 2$) oznaczenia funkcji opisujących liczbę w czasie komputerów: podatnych $S_i(t)$, zainfekowanych $I_i(t)$ i uodpornionych $A_i(t)$. Liczebność stron w czasie $t \geq 0$ opisują funkcje $R(t) = S_2(t) + I_2(t) + A_2(t)$, $B(t) = S_1(t) + I_1(t) + A_1(t)$ odpowiednio stron: Red, Blue. Zatem model z wymaganymi warunkami początkowymi dla $S_i(0) > 0$, $I_i(0) > 0$ , $A_i(0) > 0$ ($i = 1,2$) można przedstawić w postaci układu równań różniczkowych:

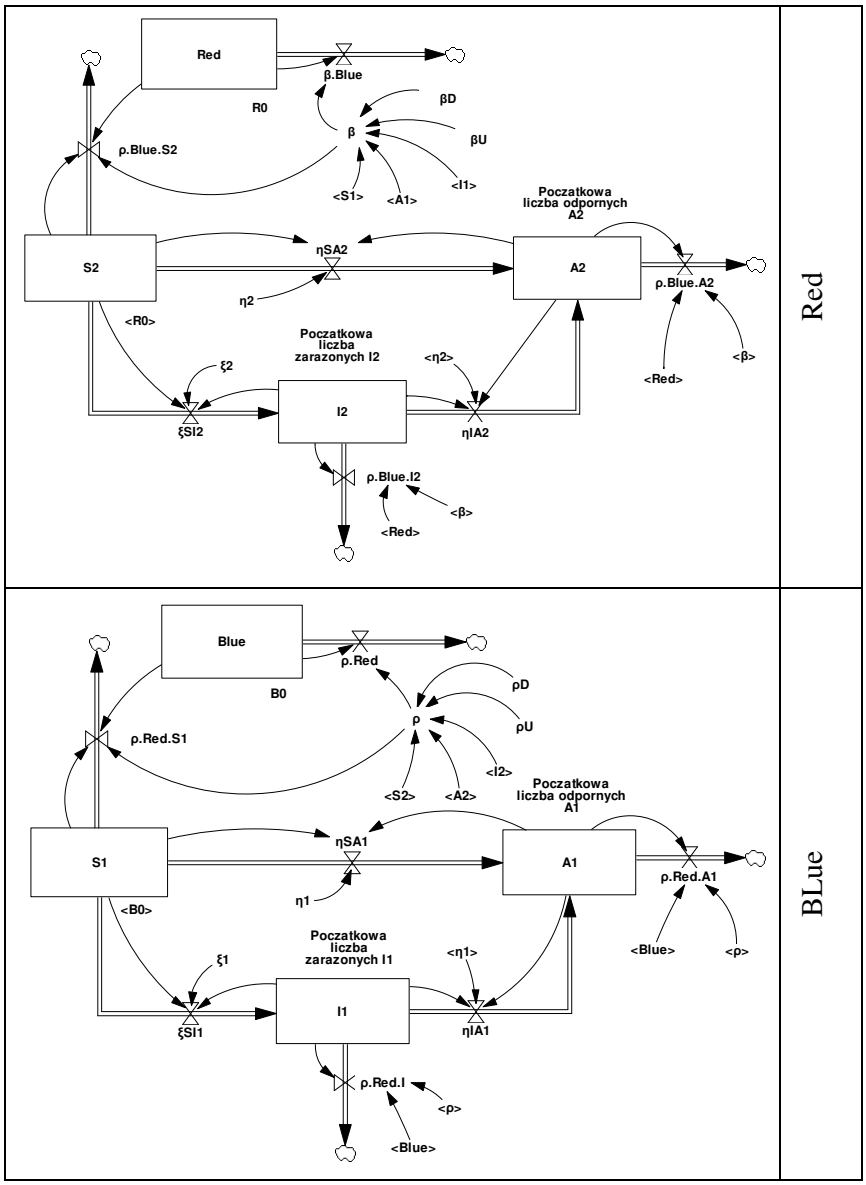
$$\frac{d}{dt} B(t) = -\rho_U \cdot \big(S_2(t) + A_2(t)\big) - \rho_I \cdot I_2(t) ,$$
$$\frac{d}{dt} R(t) = -\beta_U \cdot \big(S_1(t) + A_1(t)\big) - \beta_I \cdot I_1(t) ;$$

$$\begin{aligned}
\frac{d}{\mathrm{dt}} S_1(t) &= -\xi_1 \cdot S_1(t) \cdot I_1(t) - \eta_1 \cdot S_1(t) \cdot A_1(t) + \frac{d}{dt} R(t) \cdot \frac{S_1(t)}{B(t)} \quad , \\
\frac{d}{dt} I_1(t) &= \xi_1 \cdot S_1(t) \cdot I_1(t) - \eta_1 \cdot I_1(t) \cdot A_1(t) + \frac{d}{dt} R(t) \cdot \frac{I_1(t)}{B(t)} \quad , \\
\frac{d}{dt} A_1(t) &= \eta_1 \cdot S_1(t) \cdot A_1(t) + \eta_1 \cdot I_1(t) \cdot A_1(t) + \frac{d}{dt} R(t) \cdot \frac{A_1(t)}{B(t)} ; \\
\frac{d}{\mathrm{dt}} S_2(t) &= -\xi_2 \cdot S_2(t) \cdot I_2(t) - \eta_2 \cdot S_2(t) \cdot A_2(t) + \frac{d}{dt} B(t) \cdot \frac{S_2(t)}{R(t)} \quad , \\
\frac{d}{dt} I_2(t) &= \xi_2 \cdot S_2(t) \cdot I_2(t) - \eta_2 \cdot I_2(t) \cdot A_2(t) + \frac{d}{dt} B(t) \cdot \frac{I_2(t)}{R(t)} \quad , \\
\frac{d}{dt} A_2(t) &= \eta_2 \cdot S_2(t) \cdot A_2(t) + \eta_2 \cdot I_2(t) \cdot A_2(t) + \frac{d}{dt} B(t) \cdot \frac{A_2(t)}{R(t)} ;
\end{aligned} \tag{5}$$

$$B(t) = S_1(t) + I_1(t) + A_1(t) ,$$
$$R(t) = S_2(t) + I_2(t) + A_2(t) \ .$$

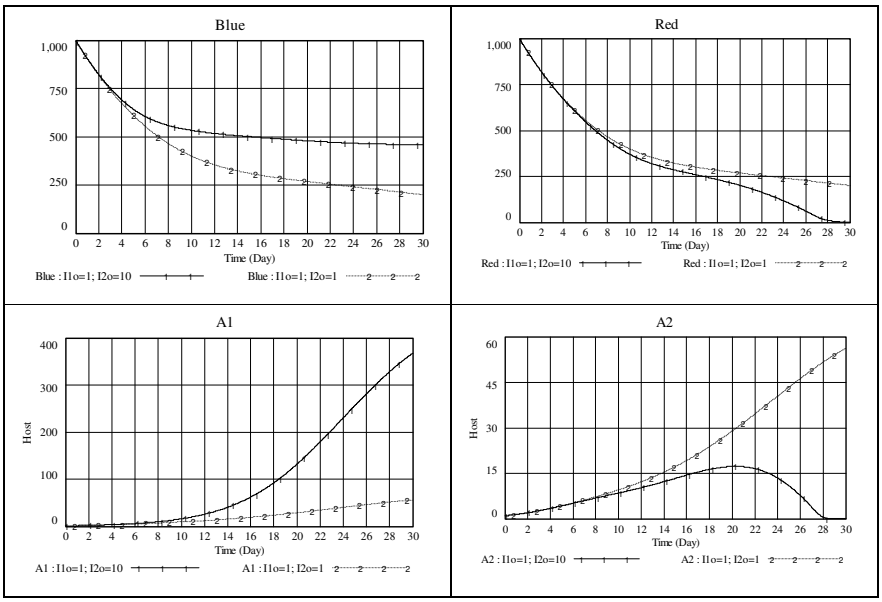
Wartości współczynników $\eta_1$, $\eta_2$, $\xi_1$, $\xi_2$, $\beta_U$, $\beta_I$, $\rho_U$, $\rho_I$ są stałe. Układ równań różniczkowych (5) ma sens w modelowaniu walki dla takiego przedziału czasu $[0, T]$, że dla każdego $t \in [0, T]$ oraz funkcje $S_i(t) > 0$, $I_i(t) > 0$ oraz $A_i(t) > 0$ ($i = 1, 2$).

Przykładowy model w języku dynamiki systemowej opisany układem równań (5) przedstawia rysunek 8, a wyniki przykładowej symulacji zostały przedstawione na rysunku 9.




*Rys. 8. Przykładowy model walki opisany układem równań (5) w ujęciu dynamiki systemowej*

*Fig. 8. An example of the combat model described by the system of equations (5) in terms of system dynamics*




*Rys. 9. Przykładowe wyniki symulacji modelu dynamiki z rys. 8*

*Fig. 9. Sample results of simulation of the combat model from Fig. 8*

## 6 Podsumowanie

Jak już wspomniano na wstępie, faktem jest to, że współczesny rozwój technologii informatycznych umożliwił prowadzenie operacji militarnych również w cyberprzestrzeni, poprzez wykorzystanie oprogramowania złośliwego. Okazuje się, że modele walki Lanchestera w połączeniu z modelami rozprzestrzeniania się kodu złośliwego można zastosować do modelowania dynamiki walki ze wsparciem operacji cybernetycznych wykorzystujących propagację kodu złośliwego w systemach przeciwnika. Najczęściej wykorzystywanymi modelami rozprzestrzenia się oprogramowania złośliwego w systemach informatycznych są modele bazujące na klasycznych modelach epidemiologicznych SIS, SIR czy SIRS i ich modyfikacji, jakim jest np. model SAI użyty w niniejszym artykule. Prezentowana w artykule metoda dynamiki systemowej nie stanowi przeszkody zastosowania innych modeli, takich np. jak: SEIRS (Mishra, Saini 2007) [23], SEIQRS (Mishra, Jha 2010) [22] i SIRA (Piqueira i Araujo 2009) [26]. Przyjęta w artykule symulacyjna metoda dynamiki systemowej pozwala modelować w ujęciu Lanchestera dynamikę działań kinetycznych ze wsparciem operacji rozprzestrzenienia się kodu złośliwego w systemach przeciwnika, uwzględniając przy tym występujące liczne sprzężenia zwrotne. Zdaniem autora, dzięki łącznemu rozpatrywaniu działań kinetycznych i cybernetycznych, jako spójnej całości w kontekście jego dynamiki systemowej, stworzone modele symulacyjne umożliwiają łatwe odwzorowanie i zrozumienie skomplikowanych relacji o charakterze nieliniowym.

Chociaż istniejące w literaturze współczesne modele symulacji procesów walki stanowią złożone modele stochastyczne, które dają wyniki lepsze niż modele Lanchestera, to jednak główną zaletą zaprezentowanych modeli jest ich prostota i łatwość rozwiązywania

układów zwyczajnych równań różniczkowych i w tym przypadku wykorzystania dynamiki systemowej do łatwego uzyskania wyników symulacji. Należy w tym miejscu zaznaczyć, że liczebność walczących stron i współczynniki strat stanowią najważniejsze czynniki mające wpływ na odwzorowanie przebiegu walki w ujęciu Lanchestera. W tym kontekście przedstawione w niniejszym artykule przykładowe modele dynamiki walki Lanchestera w połączeniu z modelem SAI, pomimo licznych uproszczeń, pozwalają na osiągnięcie zadowalających wyników symulacji.

Na zakończenie należy zaznaczyć, że w przedstawionym ujęciu połączone modele walki Lanchestera z modelami rozprzestrzeniania się kodu złośliwego, za każdym razem zapisanymi jako układy równań różniczkowych, stanowią przykład transformowania zapisu formalizmu matematycznego do graficznego języka dynamiki systemowej symulacji numerycznej. Oczywiście, w praktyce można budować modele przyrostowo bez uprzedniego formalnego i pełnego zdefiniowania układu równań różniczkowych, a opisy poziomów, przepływów i zmiennych mogą przyjmować formę samodokumentującą, znacznie odbiegającą od zapisu symbolicznego. Zatem budowa rozbudowanych i skomplikowanych modeli oraz symulacja praktycznie nie sprawia większych problemów.

Przedstawiane w artykule modele zostały zbudowane z wykorzystaniem pakietu symulacyjnego dynamiki systemowej Vensim® ver. 5.

## Literatura


1. Allen L.J.S., Burgin A.M.: Comparison of deterministic and stochastic SIS models in discrete time. *Mathematical Biosciences*, vol. 163, s. 1–33, 2000
2. Allen L.J.S.: An introduction to stochastic epidemic models. *Lecture Notes in Mathematics*, t. 1945, Springer, Berlin, s. 81–130 2008
3. Bracken J.: Lanchester models of the Ardennes campaign. *Naval Research Logistics* (NRL), Vol.42, Issue 4, s. 559-577, June 1995
4. Bracken J., Kress M., Rosenthal R.E. (red.): *Warfare modeling*. John Wiley & Sons, Inc., 1995
5. Britton T.: Stochastic epidemic models: a survey. *Mathematical Biosciences*, vol. 225, s. 24–35, 2010
6. Forester J.W.: *Industrial Dynamics*. MIT Press Cambridge, 1961
7. Forrester J.W.: *Urban Dynamics*. MIT Press Cambridge, 1969
8. Forrester J.W.: *The collected papers of Jay W. Forrester*. Wright-Allen Press, 1975
9. Hoffmann R., Protasowicki T.: Metoda dynamiki systemowej w modelowaniu złożonych systemów i procesów. *Biuletyn Instytutu Systemów Informatycznych*, vol. 12, s.19-28, 2013
10. Hoffmann R., Protasowicki T., Modelowanie pola walki z zastosowaniem koncepcji dynamiki systemowej. *Biuletyn Instytutu Systemów Informatycznych*, vol. 12, s. 29–34, 2013
11. Hoffmann R., Protasowicki T.: Klasyczne modele rozprzestrzeniania się wirusów komputerowych w ujęciu dynamiki systemowej. *Roczniki Kolegium Analiz Ekonomicznych* nr 45, 2017, s. 189-200. Szkoła Główna Handlowa, 2017
12. Kasperska E., *Dynamika systemowa. Symulacja i optymalizacja*. Wydawnictwo Politechniki Śląskiej Gliwice, 2005

13. Keeling M.J., Ross J.V.: On methods for studying stochastic disease dynamics, *Journal of Royal Society Interface*, vol. 5, s. 171–181, 2008
14. Kephart J.O, White S.R., Directed-graph epidemiological models of computer viruses. *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, s. 343–359, 1991
15. Kephart J.O, White S.R., Measuring and modeling computer virus prevalence. *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, s. 2–15, 1993
16. Kermack W.O., McKendrick A.G.: A Contribution to the Mathematical Theory of Epidemics. *Proceedings of The Royal Society*, vol. 115, s. 700–721, 1927
17. Kress M: Modeling armed conflicts. *Science*, 336 (6083) , s. 865–869, 2012
18. Kress M., Caulkins J.P., Feichtinger G., Grass D., Seidl A.: Lanchester model for three-way combat. *European Journal of Operational Research*, Vol. 264, Issue 1, s. 46-54, 2018
19. Lanchester F.W.: *Aircraft in warfare: The dawn of the fourth Arm*. Appleton New York, 1916
20. Lanchester F.W.: *The Principle of Concentration. The "N-Square" Law*. Reprint w Newman J.R. (red.): *Volume Four of The World of Mathematics*, s. 2138-2157, Simon and Schuster, New York 1956
21. Lin K.Y., MacKay N.J.: The optimal policy for the one-against-many heterogeneous Lanchester model. *Operations Research Letters*, 42 (6–7), s. 473-477, 2014
22. Mishra B.K., Jha N.: SEIQRS model for the transmission of malicious objects in computer network. *Applied Mathematical Modelling*, vol. 34, s. 710–715, 2010
23. Mishra B.K., Saini D.K.: SEIRS epidemic model with delay for transmission of malicious objects in computer network. *Applied Mathematics and Computation*, vol. 188, s. 1476–1482, 2007
24. Morse, P., Kimball, G.: *Methods of operations research*. Chapman and Hall Ltd 1951
25. Murray W.H., The application of epidemiology to computer viruses. *Computer and Security*, vol. 7, s. 139–145, 1988
26. Piqueira J.R.C., Araujo V.O.: A modified epidemiological model for computer viruses. *Applied Mathematics and Computation*, vol. 213, s. 355–360, 2009
27. Schramm H.C., Gaver D.P.: Lanchester for cyber: The mixed epidemic-combat model. *Naval Research Logistics* (NRL) Vol.60, Issue7, s. 599-605, October 2013
28. Sterman J.D.: *Business Dynamics. Systems Thinking and Modeling for a Complex World*. McGraw-Hill, 2000
29. Tolk A.: Modeling effects. w: Tolk A. (red.): *Engineering principles of combat modeling and distributed simulation*. Hoboken, JohnWiley & Sons, Inc. s. 145-170, 2012
30. Washburn A., Kress M.: *Combat modeling*. Springer-Verlag 2009

## Streszczenie

Współczesny rozwój technologii informatycznych umożliwił prowadzenie operacji militarnych w cyberprzestrzeni z wykorzystaniem oprogramowania złośliwego. Okazuje się, że modele walki Lanchestera w połączeniu z modelami rozprzestrzeniania się kodu złośliwego można zastosować do ilościowego modelowania operacji kinetycznych wspartych operacjami propagacji kodu złośliwego w systemach przeciwnika. W pracy przedstawiono w ujęciu dynamiki systemowej dwa modele walki z użyciem kodu złośliwego oraz przykładowe wyniki ich symulacji. Modele w języku dynamiki systemowej bazują na klasycznym modelu dynamiki walki bezpośredniej Lanchestera oraz modelu propagacji kodu złośliwego w systemach komputerowych SAI (ang. *susceptible, antidotal, infected*).

**Słowa kluczowe**: dynamika systemowa, model dynamiki walki, model Lanchestera, model propagacji kodu złośliwego, SAI

# Modeling in the language of system dynamics of cyber operations using combat models combined with models of spreading malicious code

## Summary

Modern information technologies have enabled to carry out military operations in cyberspace with using malware. It turns out that Lanchester combat models in conjunction with the models of malicious code propagation in IT systems can be used for quantitative modeling of kinetic operations supported by cyber operations with malware propagation in opposing forces' IT systems. This paper presents in terms of system dynamics two combat models with using propagation of malware codes and the sample results of their simulation. The system dynamics combat models are based on the Lanchester classical direct fire combat model and SAI (susceptible, antidotal, infected) model of malicious code propagation in computer systems.

**Keywords**: system dynamics, combat model, Lanchester model, malicious code propagation model, SAI