2013-08-12

# Lanchester for Cyber: The Mixed Epidemic-Combat Model

Schramm, Harrison C.; Gaver, Donald P.

Monterey, California: Naval Postgraduate School.

Published online 7 October 2013 in Wiley Online Library (wileyonlinelibrary.com).
http://hdl.handle.net/10945/37796

# Lanchester for Cyber: The Mixed Epidemic-Combat Model

**Harrison C. Schramm, Donald P. Gaver**

*Operations Research Department, Naval Postgraduate School*

Received 28 November 2012; revised 29 April 2013; accepted 12 August 2013
DOI 10.1002/nav.21555
Published online 7 October 2013 in Wiley Online Library (wileyonlinelibrary.com).

**Abstract:** Future conflict between armed forces will occur both in the physical domain as well as the information domain. The linkage of these domains is not yet fully understood. We study the dynamics of a force subject to kinetic effects as well as a specific network effect–spreading malware. In the course of our study, we unify two well-studied models: the Lanchester model of armed conflict and deterministic models of epidemiology. We develop basic results, including a rule for determining when explicit modeling of network propagation is required. We then generalize the model to a force subdivided by both physical and network topology, and demonstrate the specific case where the force is divided between front- and rear-echelons. © 2013 Wiley Periodicals, Inc. Naval Research Logistics 60: 599–605, 2013

**Keywords:** campaign analysis; Lanchester equations; epidemic model

## 1. INTRODUCTION

The domains of conflict are constantly evolving, and with them, the analytic methods to understand, prepare, and hopefully prevent conflict. Lanchester's original (1916) [14] equations were in response to a (then) revolutionary change in warfare—aircraft. Today, we sit poised on the beginning of a new revolution: addition of the cyber domain. This change needs to be understood in order to shape both acquisition and operational strategies.

We focus our effort on the analysis of a large ground combat force using a peer-to-peer (P2P) network susceptible to cyber-infection. In our analysis malicious code, which we henceforth collectively call malware, is introduced and spread between tactical devices with the effect of reducing its hosts' combat effectiveness. Accordingly, the force considered will simultaneously contend with kinetic combat effects, which we model as Lancheter aimed-fire, and cyber effects, which we model as an epidemic process.

Our major contribution is to unify these classic ideas and analyze the resulting model. Both structures have been studied independently and are independently well understood; we propose and analyze the combined model. The goal is both a better understanding of an important combat environment as well as a deeper understanding of the trade-offs between cyber and kinetic capabilities.

We focus on an extension of the general, or Susceptible-Infected-Removed ($S - I - R$) epidemic as developed by Kermack and McKendrick [12], treating the simple, or $S$–$I$, epidemic as an included case. We then combine it with Lanchester's aimed fire and area fire models. Similarly, other variants of attrition action such as area fire or mixed effects (i.e., Deitchman's Ambush model) may be developed following our approach.

Our article is structured as follows: In Section 2, we review relevant work. In Section 3, we develop our model. In Section 4, we present some analytic and numerical results. In Section 5, we extend our model to include nonhomogeneous mixing and combat effects, and in section 6, we develop the model for area fires.

## 2. LITERATURE REVIEW

Deterministic combat models are a staple of Military Operations Research; for an overview see [20, 9, 2]. Instantaneous malware spread in generalized Lanchester systems is explored in [19]. For an overview of epidemic models, see [6]. In particular, nonhomogeneous mixing models, as presented in Section 5, are addressed in [8, 13, 18]. A more recent approach to epidemics may be found in [15]. Previous authors have considered the spread of information, which malware may be considered, in a military/national security context. See Richardson [16, 17] as well as Bettencort et al. [1]. Each of these authors consider the effect of ideas and epidemics, but do not consider the spread of ideas "weaponized" the same way we treat malware in our development.

Malware spread on wireless networks is considered in [10]. Several articles by Jamil and Chen, notably [11], address the

*Correspondence to:* H.C. Schramm (hcschram@nps.edu)

spread of malware on networks as an S-I process with heterogeneous mixing. The specific case of epidemic S-I spread on Mobile Ad-Hoc Networks (MANETS) is considered both in [3] and [5].

Our approach breaks from the traditional models of infectious disease in two important ways. The classic model of a general epidemic, the $S-I-R$ model introduced by Kermack and McKendrick [12], assumes that members of the population become infected through contact with infected members, and then are removed from the infected population, through recovery or death, after some exponentially distributed time independent of the number of removals. Thus, the Removeds, in class $R$ are a bookkeeping variable to track the total number in the class and are not "active" in the same way as the Infecteds ($I$). In our development, both class $I$ and class $R$ act upon the other members of the population. Members of class $R$ are active and are in competition with class $I$. The dynamics captured by this competition dynamic shows the real-world "race" between malware and patches. The idea of an epidemic-pushed patch is important when considering the management of a MANET because information is shared only via P2P connections. In our model, fighters are attrited, that is, killed by the Red force, at rate linearly dependent on the size of the red force, $Z$ and in the area fire case also dependent on the Blue force $B$. The second departure is that the total population, $N$, is not static due to attrition from red fighters. Classic analysis of the $S-I-R$ model rests on the fact that $N = S+I+R$ for all times, and therefore, a degree of freedom may be removed. In our analysis, the attrition of the blue force is as much of interest as the epidemic process.

## 3. FORMULATION

We now make our thoughts about simultaneous conflict in both the cyber and kinetic domains concrete. A Blue force, $B$, is subject to simultaneous malware infection and kinetic battle. The blue force is subdivided into three cohorts with regard to malware; further refinements with respect to distance from the battlefront follow in Section 5. This blue force is in a Lanchester–aimed fire battle with the Red Force, $R$, which is monolithic with respect to malware.

*Susceptible - class* S Susceptible blue fighters are those who have not been infected by the malware nor the cure (patch). They are noted as class $S$, with the variable $S(t)$. On exposure to members of class $I$, they may become infected at rate $\eta$. Likewise, on exposure to patched fighters (class $R$), they may be patched and permanently immune to the cyber infection. Class $S$ fighters have an effectiveness of $\beta_U$ (for $\beta$ "UP") relative to the red force.

*Infected - class* I Infected blue fighters are those who currently have the cyber infection, with the variable $I(t)$. They have effectiveness $\beta_D$ for $\beta$ "Down" relative to the Red force with the understanding that $\beta_D \leq \beta_U$. Blue fighters become infected from class $S$ only, as noted above.

*Removed - class* R Blue fighters, either $S$ or $I$, become patched or removed via contact with members of class $R$ with variable $R(t)$. Members of class $R$ have effectiveness of $\beta_U$ relative to the red force and are no longer at risk for cyber infection.

*Red Force* Red fighters (denoted by $Z$) are monolithic, in the sense that they are not vulnerable to a cyber infection. They have a single, uniform effectiveness parameter in attriting the blue force of $\rho$.

When referring to the Blue force *en masse*, we use the notation $B(t)$, with the understanding that $B(t) = S(t) + I(t) + R(t)$.

### 3.1. Infection Process: Model Options

We now pause to ask a fundamental question: what mechanism spreads malware among the blue fighters? Malware is different than biological pathogens because it is "disease by design"; the rule-sets for spread and duration of action are limited only by the imagination and programming skill of the designer; for an example of the real life complexities of malware, see [7]. While there are potentially limitless spread mechanisms, we highlight three that may be both operationally interesting and analytically tractable via differential equation methods:

*"Lanchster" infection* It is possible that infection spreads at a rate dependent on $I$ alone. This particular mechanism makes malware like aimed fire and implicitly assumes that an infected computer may always find—and infect—an uninfected computer.

*Kermack–McKendrick infection* Infection may spread at a rate dependent on the product $SI$, the "classic" $SIR$ model.

*Daley–Kendall infection* It is also possible that malware may have rules, such as "if another infected unit is encountered, cease infection." This is similar to the mechanism proposed by Daley and Kendall [4] for the analysis of rumor spread and may have important implications, particularly if the adversary (red force) is balancing the breadth of spread with avoiding detection.

Our analysis will focus exclusively on the Kermack–McKendrick-like infection. Similarly, there are three common varieties of Lanchester models:

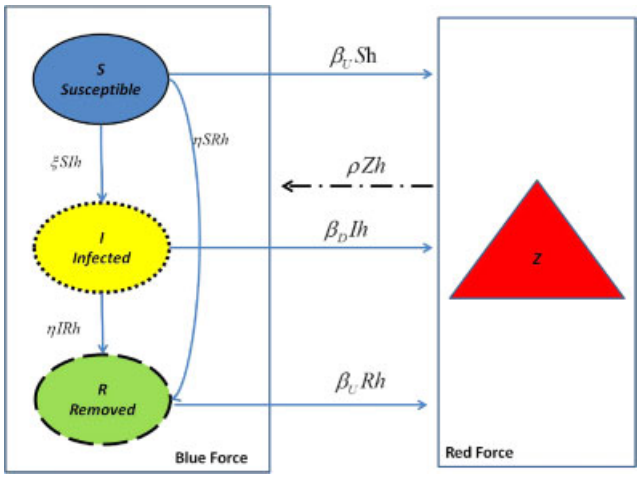


**Figure 1.** A depiction of the internal epidemic process and external Lanchester process. The ovals depict the interaction due to the malware epidemic, whereas the squares depict the action of the force as a whole. The red force is monolithic and has no interior dynamics. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

*Aimed Fire* Fighters on either side attrite their adversary at a rate dependent on the number of fighters on their side only. This is called aimed fire because it implicitly assumes that each active fighter may find an adversary to target.

*Area Fire* Fighters on either side attrite their adversary at a rate dependent on the number of fighters on both sides. This is called area fire because attrition depends both on the number of shooters and the density of targets presented. Hybrids between aimed and area fire exist, and are handled with fractional exponents, see [9].

*Mixed effects* Fighters on one side use aimed fire, and their adversary uses area fire.

These three models are developed and exercised with an instantaneous infection in [19]. Our analysis will focus exclusively on aimed fire, where we believe that malware is most important. Malware reduces the quality of connectivity and information; we choose to illustrate it in an aimed-fire context.

### 3.2. State Transitions

During any infinitesimal time period, $h$, the following events may occur:

- $S \to I$ at rate $SI\xi h$
- $S \to R$ at rate $SR\eta h$
- $I \to R$ at rate $IR\eta h$
- Blue fighter attrited at rate $\rho Zh$, weighted per-class; for example, $\rho Z \frac{S}{S+I+R} h$
- Red fighter attrited at rate $[\beta_U (S+R) + \beta_D I]\, h$

For a summary, see Fig. 1. Upon taking limits, we produce the following differential equation model,

$$\begin{aligned}
\frac{dS}{dt} &= -\xi SI - \eta SR - \rho Z \frac{S}{S+I+R} \\
\frac{dI}{dt} &= \xi SI - \eta RI - \rho Z \frac{I}{S+I+R} \\
\frac{dR}{dt} &= \eta (SR + IR) - \rho Z \frac{R}{S+I+R} \\
\frac{dZ}{dt} &= -\beta_U (S+R) - \beta_D I.
\end{aligned} \tag{1}$$

A typical instantiation of Eqs. (1) is shown in Fig. 2.

## 4. ANALYSIS

### 4.1. Preliminaries

It is clear that should the blue force win, in the sense that $Z(\infty) = 0$, then $S(\infty)$ and $I(\infty)$ will also equal 0, and $B(\infty) = R(\infty)$.

A feature of interest for the epidemic process is the maximum size of the epidemic in the absence of attrition. We disregard the $\frac{dZ}{dt}$ equation in (1) and focus on the first three expressions, when $\rho = 0$. We may take advantage of the fact that in this specific case

$$B = S + I + R, \tag{2}$$

along with the fact that we have set $\beta = \rho = 0$ to eliminate any combat effects, we may exclude the $Z$ variable. In the particular case where the patch and malware spread via similar mechanisms, therefore, letting $\xi = \eta$, and appropriate substitution of (2) into (1), the system has a closed-form solution,

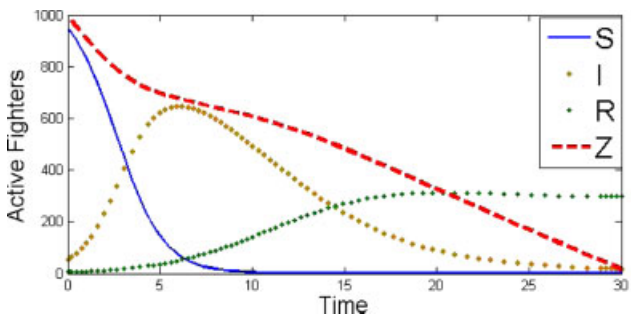


**Figure 2.** A typical instantiation of the Lanchester-epidemic model, with the following parameters: $\xi = .001, \eta = .0005, \rho = .05, \beta_U = .1, \beta_D = .01$. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

$$
\begin{aligned}
S(t) &= \frac{B(0)\,S(0)}{S(0)+(B(0)-S(0))\,e^{\xi B(0)t}} \\
I(t) &= \frac{B(0)^2 I(0)}{\left(S(0)+(B(0)-S(0))\,e^{\xi B(0)t}\right)\left(R(0)+(B(0)-R(0))\,e^{-\xi B(0)t}\right)} \\
R(t) &= \frac{B(0)\,R(0)}{R(0)+(B(0)-R(0))\,e^{-\xi B(0)t}}.
\end{aligned} \tag{3}
$$

It follows that the time of maximum infection is given by:

$$
t_{I_{\text{Max}}} = \frac{1}{2\xi B(0)} \ln\left[\frac{(B(0)-R(0))\,S(0)}{(B(0)\,R(0)-R(0)\,S(0))}\right], \tag{4}
$$

from which the magnitude of greatest infection may be obtained.

### 4.2. Time Scaling

When do epidemic effects of malware need to be explicitly considered in a unified combat model? If the spread of the cyber infection is very fast compared to the combat process —for example, if the time until malware saturation is $100\mu s$ and the rate of blue attrition due to red action is on the order of 1 per min—then the disruption of the network may be adequately treated as a uniform, catastrophic failure; this situation is described in [19]. Alternatively, if the spread of cyber infection is very slow, then the effect may be negligible and the attrition formulation alone is sufficient.

We make the following observation: in order for both the cyber and kinetic effects to be of interest, the rate of blue fighters leaving class $S$ due to cyber effects should be on the same order of magnitude as the rate of blue fighters being lost to casualties. If the initial blue force is $B_0$, it is clear that the instantaneous rate of infection is always less than or equal to $\xi B_0^2/4$, and the full model is most interesting in cases where

$$
\frac{(\beta_{\text{U}}-\beta_{\text{D}})\,\xi S^2(0)}{4\beta_{\text{U}}\rho Z(0)} \approx 1, \tag{5}
$$

which is to say that the loss in effectiveness for the blue side due to cyber effects is on the same order as loss in effectiveness from kinetic attrition. For cases where $(\beta_{\text{U}}-\beta_{\text{D}})\,\xi S^2(0) >> 4\beta_{\text{U}}\rho Z(0)$, the cyber effects occur very quickly relative to the battle and it is appropriate to model the effect as instantaneous. Similarly, if $(\beta_{\text{U}}-\beta_{\text{D}})\,\xi S^2(0) << 4\beta_{\text{U}}\rho Z(0)$, the cyber infection spreads so slowly as to be negligible in comparison to the combat process, and may be ignored.

### 4.3. Pure Epidemic Versus Aimed Fire

If we let $\eta = 0$, $\beta_{\text{D}} = 0$, and $\rho = 0$, the result is that the red force uses an epidemic to disable the blue force, and the blue force uses aimed fire. Eqs. (1) reduce to:

$$
\begin{aligned}
\frac{dS}{dt} &= -\xi SI \\
\frac{dI}{dt} &= \xi SI \\
\frac{dZ}{dt} &= -\beta_{\text{U}} S,
\end{aligned} \tag{6}
$$

and $B(t) = S(t) + I(t)$. We use the fact that $S(t)$ has a closed form solution,

$$
S(t) = B(0) - \frac{I(0)\,B(0)}{I(0)+S(0)\,e^{-\xi B(0)t}},
$$

which we may substitute and solve to find an explicit solution for $Z$,

$$
Z(t) = \max\left(0, Z(0) - \frac{\beta}{\xi}\ln\left[\frac{B(0)}{I(0)+S(0)\,e^{-\xi B(0)t}}\right]\right), \tag{7}
$$

from which immediately follows:

$$
Z(\infty) = \max\left(0, Z(0) - \frac{\beta}{\xi}\ln\left(\frac{B(0)}{I(0)}\right)\right). \tag{8}
$$

Recalling that by definition, $B(t) \geq I(t)\,\forall_t$, we are guaranteed that the last term in Eq. (8) will be negative. It has the natural interpretation of losses inflicted by the blue side. Equation (8) allows for quick consideration of the tradeoffs between kinetic and nonkinetic effects and determines the final condition, $B(\infty), Z(\infty)$ in terms of initial conditions and parameters.

### 4.4. Time Until Patch Relsease

We may also ask "how long after the cyber infection is introduced will the blue side release a patch?" This question raises two issues: first, the time of spread before detection, and second, the time to develop and deploy an effective patch. A straightforward approach is to use the saturation percentage of the simple epidemic; we may define a saturation level to be reached before the blue force begins developing a patch; if we define this value as $\alpha$, $0 < \alpha < 1$, the time that $\frac{I}{B} = \alpha$ is given by:

$$
T_1(\alpha) = \frac{1}{\xi B(0)}\ln\left(\frac{\alpha B(0)\,(B(0)-I(0))}{I(0)}\right). \tag{9}
$$

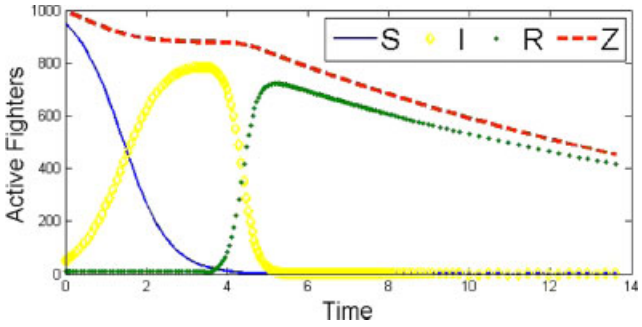


**Figure 3.** An example of delayed patching. The infection spreads until 50% of the population is infected, at approximately $T = 1.6$. Then, two time periods later, a patch is deployed. This approach illustrates trades between time to detect, time to develop patch, and time to deploy patch. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

Equation (9) does not account for combat losses; if the blue force is large and losses are homogeneous across the field, this is not a critical concern. Although noting this deficiency, we may treat (9) as a simple metric for malware detection. Once malware has been detected, there is a latency time, $T_L$ , that it takes the blue force to develop and deploy a patch. We treat this parametrically as a fixed quantity; other refinements are possible. The goal is to be able to compare speed of detection, rate of patch development, and rate of patch dissemination under a single metric. Rate of patch dissemination and network administrator decisions become especially important when considering a nonhomogeneous force, as in Section 5. Using this framework, we may examine the consequences numerically, see Fig. 3.

## 5. NONHOMOGENEOUS MIXING

In principle, we may subdivide either force in as many subsets as we desire, with inter and intra mixing parameters. As an illustrative example, we subdivide the blue force into two groups: the front-line troops, which we subscript with $F$, and the rear-echelon troops, we subscript with $N$. For simplicity, we assume the infection and patch spread via the same pathways, that is, $\eta = \xi$. We do not assume that the rate of communication from the front to the rear is equal to the rate of communication from the rear to the front. Finally, we group the adversaries' preference for attacking the parts of the force as $\rho_{\mathrm{F}}$ and $\rho_{\mathrm{N}}$, and we retain the notation $\beta_{\mathrm{U}}$ and $\beta_{\mathrm{D}}$ for "up" and "down" fighters. A diagram of this situation is presented in Fig. 4.

In general, these equations take the form,

$$\begin{aligned}
\frac{dS_j}{dt} &= -S_j\left(\xi_{1j}I_1 + \ldots + \xi_{mj}I_{mj}\right) \\
&\quad - S_J\left(\xi_{1j}R_1 + \ldots + \xi_{mj}R_{mj}\right) - \left(\rho_j\right) Z\frac{S_j}{S_j + I_J + R_j} \\
\frac{dI_j}{dt} &= S_j\left(\xi_{1j}I_1 + \ldots + \xi_{mj}I_{mj}\right) \\
&\quad - I_J\left(\xi_{1j}R_1 + \ldots + \xi_{mj}R_{mj}\right) - \left(\rho_j\right) Z\frac{I_j}{S_j + I_J + R_j} \\
\frac{dR_j}{dt} &= S_j\left(\xi_{1j}R_1 + \ldots + \xi_{mj}R_{mj}\right) \\
&\quad + I_J\left(\xi_{1j}R_1 + \ldots + \xi_{mj}R_{mj}\right) - \left(\rho_j\right) Z\frac{R_j}{S_j + I_J + R_j} \\
\frac{dZ}{dt} &= -\sum_j \left[\left(S_j + R_j\right)\beta_{\mathrm{U}j} + I_j\beta_{\mathrm{D}j}\right]. \qquad (10)
\end{aligned}$$

We introduce four mixing parameters: $\xi_{\mathrm{FF}}, \xi_{\mathrm{FN}}, \xi_{\mathrm{NN}}, \xi_{\mathrm{NF}}$. For example, $\xi_{\mathrm{FN}}$ is the mixing from the front to the rear. Our model now has seven classes–six of blue and one of red.

If we presume that the malware enters at the rear echelon, it may be suppressed by slowing communication from the rear to the front. The opposite situation is true of patches, which may tend to originate at the rear. Therefore, different cross-cohort communication schemes are advantageous for different phases of the cyber/kinetic conflict. For an example of the effect of the distribution of patched fighters in determining the outcome of the battle, compare Fig. 5a with Fig. 5b.

## 6. AREA FIRES

Although we feel that aimed fire is the most interesting case for cyber-effects, we complete our exposition by discussing the case of an area fire implementation. In the original aimed fire case (1), the final term is of the form

$$-\rho\frac{ZS}{S + I + R},$$

where $\frac{S}{S+I+R}$ is a correction factor accounting for the fractional (per-group) exposure to red's fire. In area fire, the

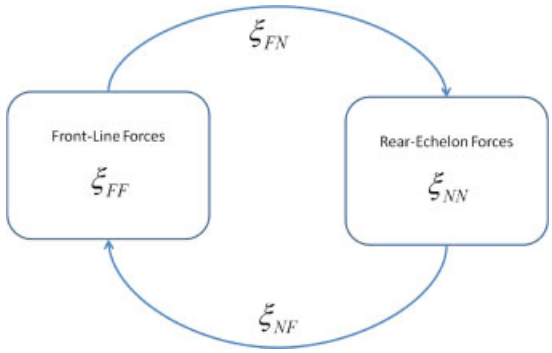


**Figure 4.** A block diagram of the mixing between forces. Each force transmits messages within its class and across classes. The subscripts are read "from A to B"; so $\xi_{\mathrm{FN}}$ is the transmission rate from the front to the rear. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

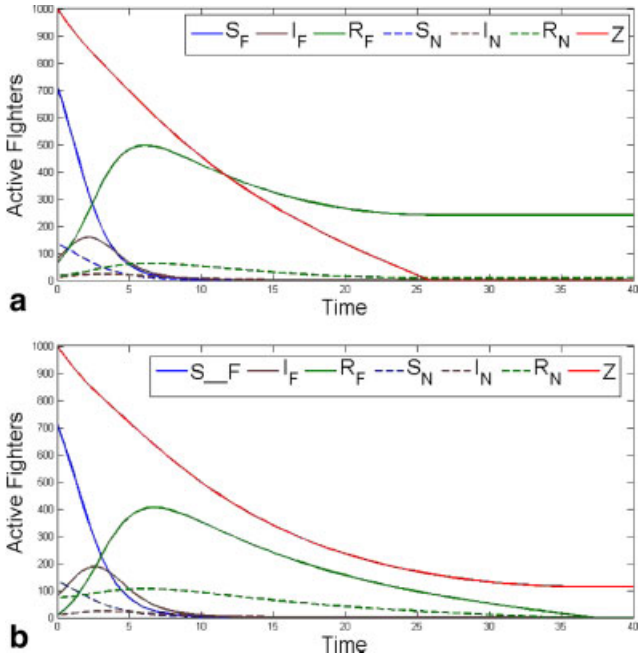


**Figure 5.** Two cases of nonhomogeneous mixing, demonstrating the dramatic effect that the distribution of initial patches has on the outcome of the battle. In both examples, $\xi_{FF} = \xi_{NN} = .001, \xi_{FN} = \xi_{NF} = .0005, \beta_{UF} = .09, \beta_{UN} = .063, \beta_D = 0, \rho_F = .06, \rho_N = .018$. (a) Epidemic Lanchester combat with nonhomogeneous mixing. In this example, the blue force is divided into two partitions, Front $F$ and Rear $N$, with 80% at the front initially at the front and 20% of the force at the rear. Initial infections consist of 10% of the front-line force and 5% of the back-line force at $t = 0$. 64 fighters both in the front and 16 fighters in the back have the patch installed at $T = 0$. (b) A second example of Epidemic Lanchester combats with nonhomogeneous mixing. This time, the 80 patched fighters are redistributed with 8 on the front line and 72 in the rear. This example illustrates the leverage of patched fighters placement. [Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

magnitude of attrition is the product of the red and blue forces *en masse*, leading to

$$-\rho \frac{ZS}{S+I+R}(S+I+R) = -\rho ZS.$$

The resulting area fire model is:

$$\begin{aligned} \frac{dS}{dt} &= -\xi SI - \eta SR - \rho_R SZ \\ \frac{dI}{dt} &= \xi SI - \eta IR - \rho_R IZ \\ \frac{dR}{dt} &= \eta SR + \eta IR - \rho_R RZ \\ \frac{dZ}{dt} &= -\beta_U SZ - \beta_U RZ - \beta_D IZ, \end{aligned} \tag{11}$$

where we have introduced the notation $\rho_R$ to remind us that the area fire coefficient is not that same as for aimed fire. Perhaps surprisingly, much of our prior analysis is unchanged. The time of maximum infection found in Eq. (4) does not change. The recommended threshold for specifically studying cyber effects, Eq. (5) is changed slightly; for area fire it becomes

$$\frac{(\beta_U - \beta_D)\,\xi S^2 S(0)}{4\beta_U \rho Z(0) B(0)} \approx 1. \tag{12}$$

The estimates of the time to patch in Section 4.4 are unchanged as well. Finally, the comparison of pure-cyber versus pure-kinetic effects of Section 4.3 may be made for this model as well. Following the same logic that led to Eq. (7) may be applied, yielding

$$Z(t) = Z(0)\left[\frac{B(0)}{I(0) + S(0)\,e^{-\xi B(0) t}}\right]^{-\beta/\xi}, \tag{13}$$

and

$$Z(\infty) = Z(0)\left[\frac{B(0)}{I(0)}\right]^{-\beta/\xi}. \tag{14}$$

## 7. CONCLUSIONS

We have described the problem of combat with simultaneous cyber and kinetic dimensions, formulated a model based on one set of choices for cyber- and kinetic- conflict, and derived analytic results, to include a rule for determining when detailed study of the cyber dynamic is required and when it is not. We also include results highlighting the competition aspect of spreading malware and counter-spreading patches. Our goal has been to stimulate thought from the analytic community and provide a set of baseline results to scope more complex efforts. The methodology presented here may be applied to other choices with regard to both the malware spread and Lanchester attrition.

One next step for this research is to consider stochastic effects, which are not brought out in this first, exploratory paper. We expect that a stochastic treatment will bring out additional behaviors, and will be particularly useful when the number of initial malware carriers is small. For example, a stochastic treatment will allow us to consider the possibility that one or several initial malware carriers are attrited by the red force - a possible outcome which our deterministic model presented here does not allow. This might lead to operational insights for the joint employment of cyber and kinetic warfare.

Another step for this research is to consider other types of networks; we have assumed mobile networks with volatile connections, so the assumption of a mass-action epidemic

is acceptable. With specified network topologies, different results may be obtained, and the structure of the network may be part of the decision space for both sides. We hint at this type of result in Section 5, but a fuller treatment is needed.

## REFERENCES


[1] L. Bettencort, A. Cintron-Arias, D. Kaiser, and C. Castillo-Chavez, The power of a good idea: Quantitative modeling of the spread of ideas from epidemiological models, Phys A Stat Mech Appl 364 (2006), 513–536.

[2] J. Bracken, M. Kress, and R. Rosenthal, Warfare modeling, MORS, Alexandria, Virginia, 1995.

[3] P.Y. Chen and K.C. Chen, Information epidemics in complex networks with opportunistic links and dynamic topology, IEEE Global Telecommunications Conference, Miami, Florida, 2010.

[4] D.J. Daley and D.G. Kendall, Stochastic rumours, IMA J Appl Math 1 (1965), 42–55.

[5] M. Draief, A. Ganesh, and L. Massoulie, Thresholds for virus spread on networks, Ann Appl Probab 18 (2008), 359–378.

[6] D. Daley and J. Gani, Epidemic modeling, Cambridge University Press, England, 1999.

[7] N. Falliere, L.O. Murchu, and E. Chien, W32. Stuxnet Dossier: Version 1.4 (February 2011). Cupertino, CA: Symantec Corp, 2011.

[8] J. Gani, A simple deterministic epidemic in several related growing communities, J Appl Probab 31 (1994), 17–25.

[9] D.S. Hartley, Predicting combat effects, INFORMS, Hanover, MD, 2001.

[10] H. Hu, S. Myers, V. Colizza, and A. Vespignami, WiFi networks and malware epidemiology, Proc Natl Acad Sci USA 106 (2009), 1318–1323.

[11] T. Chen and N. Jamil, Worm epidemiology, China Commun 3 (2006), 27–31.

[12] W. Kermack and A. McKendrick, A contribution to the mathematical theory of epidemics, Proc R Soc London Ser A 115 (1927), 700–721.

[13] M. Kress, The effect of social mixing controls on the spread of smallpox - a two-level model, Health Care Manag Sci 8 (2005), 277–289.

[14] F.W. Lanchester, Aircraft in warfare: The dawn of the fourth Arm, Appleton, New York, 1916.

[15] M.E. Newman, Networks: An introduction, Oxford University Press, Oxford, 2010.

[16] L. Richardson, War moods I., Psychometrika 13 (1948), 147–174.

[17] L. Richardson, War moods II., Psychometrika 13 (1948), 197–219.

[18] S. Rushton and A. Mantner, The deterministic model of a simple epidemic for more than one community, Biometrika 42 (1955), 126–132.

[19] H. Schramm, Lanchester models with discontinuities: An application to networked forces, Mil Oper Res 17 (2012), 59–68.

[20] A. Washburn and M. Kress, Combat modeling, Springer, New York, 2009.