Better Timing of Cyber Conflict*

Elisabeth Paulson† Christopher Griffin†

ABSTRACT

In this paper, we construct a model of cyber-weapon deployment and attempt to determine an optimal deployment time for cyberweapons using this model. We compare and contrast our approach to that in Axelrod and Iliev (R. Axelrod and R. Iliev. Timing of cyber conflict. Proceedings of the National Academy of Science, (1322638111), 2013.), showing that our model accurately captures four real-world scenarios and has fewer quantities that are difficult to measure than the aforementioned approach. Under simplifying assumptions, we prove rules of thumb for determining when and wether a cyber-weapon should be deployed.

I INTRODUCTION

Cyber-attacks are the malicious use of computer and network technology for the purpose of damaging or destroying infrastructure or human life. In their current state, cyber-attacks may be regarded as either cyber-warfare or cyber-terrorism. Cyber-terrorism is defined by Lewis [1] as "...the use of computer network tools [by a non-governmental organization] to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population." Cyber-warefare, conversely, can be divided into two types: cyber espionage and cyber-attacks both of which are conducted by governments using paid hackers [2]. Cyber-espionage involves the use of computer resources to steal information, while cyber-attacks have the same stated goal as cyber-terrorism except they are conducted by a formal "cyber-army" of the attacking government and (should) be used against legitimate military targets in accordance with the laws of war. The United States Director of National Intelligence (DNI) defines cyber-attacks as the more serious threat [2], and states that in general cyber-security (i.e., defense against cyber-attack) is the most critical challenge for the United States [3].

Cyber-attacks are frequently in the popular press, with Stuxnet and its related attacks Flame, Duqu and Gauss being the most recent and extreme example of a massive cyber-attack allegedly[1] conducted by a government or governments against Iran [4]. Many consider this to be the very first example of cyber-warfare conducted by one country or coalition against another [5] and Milevski asserts that the Stuxnet deployment was an example of Special Operations on the cyber-battlefield [6].

The presence of sophisticated cyber-weapons (where we stipulate that Stuxnet was a sophisticated cyber-weapon) raises several questions on the ethics of their use [7]. It also creates a set of new optimization questions for the use of cyber-weapons. Unlike conventional weapons, cyber-weapons become obsolete with the discovery of exploits and the dissemination of patches. Therefore, either a country or group must engage in continuous development of new weapons for cyber-space or they must be prepared to deploy these weapons immediately upon creation. On the other hand, weapons like Stuxnet are only useful as long as they remain covert, therefore any deployed weapon like Stuxnet can only be expected to provide a return on investment (ROI) for a finite period of time, again (intuitively) encouraging early deployment. On the other hand, cyber-attacks (including hacking) can lead to substantial losses when they are discovered. By way of example, consider the hacking scandal surrounding the German Chancellor's phone [8]. This alleged cyber-attack has led to diminished relations between the United States and Germany leading to the question: under what conditions do the costs of a cyber-attack outweigh the benefits?

Axelrod and Iliev [9] attempt to answer some of these questions by posing a mathematical model of the benefit of deploying cyber-weapons at a certain time. In this paper, we analyze Axelrod and Iliev's model and

*Portions of this work were supported by Applied Research Laboratory Exploratory and Foundational Research Funding.

†Communications, Information and Navigation Office, Applied Research Laboratory, Penn State University, University Park PA, 16802. E-mail: ecp141@psu.edu, griffinch@ieee.org

[1]Responsibility for these attacks has never been formally assumed by any government. All responsibility still remains alleged.

argue that it is an excellent start, but incomplete and failing to sufficiently take into account long-term payoff or loss (as may have occurred in both Stuxnet and the hacking of German Chancellor's phone). In particular, one of the failures of their model is a lack of proper definition of stakes as well as gains and a failure to explicitly include loss. We propose an enhancement to the their model that takes these factors into consideration and then analyze the same examples as those given by Axelrod and Iliev in the light of our improved model. A major take-away from our model is that under simplifying assumptions we can determine criteria for when a cyber-weapon should be deployed immediately vs. never deploying the weapon. For more complex models of payoff (e.g., Martingale models) we show that deployment times may vary substantially within a given time horizon.

1 RELATED WORK

The problem of timing in releasing a cyber-weapon is qualitatively similar to several problems that already exist in the literature. The weapon-target assignment problem [10] is a well known NP-hard optimization problem whose solution yields an optimal targeting plan for a set of weapons against a set of (known) targets. This optimization problem does not consider the problem of when to release (as it is assumed that release will occur immediately after planning). Time games are a related area of game theory [11]. These games include attrition games, in which one player must decide when to retire [12]. Another class of timing games are duel games in which the players have a set of bullets (in the simplest games, one bullet) and must decide when to fire based on changing accuracy. Surveys of these games are given in [13] and [14]. None of these timing games precisely relates to our problem, where we do not have an accurate model of the opponent's strategy set. Thus, our problem is more closely related to a weapon-target assignment problem with the decision of when to fire being paramount.

2 PAPER ORGANIZATION

The remainder of this paper is organized as follows: In Section II we discuss the elements of the model of Axelrod and Iliev and present our variation to this model. In Section III we use our model with simple (non-stochastic) models of gains and losses associated with deploying a cyber-weapon. In Section IV we analyze our model when the gain associated with the cyber-weapon follows a random walk (like a non-drifting stock). In Section V we compare our findings to real-world events and the analysis in [9]. Finally, we present conclusions and future directions in Section VI.

II MATHEMATICAL MODEL

We begin by discussing the model of Axelrod and Iliev: in this model, a quantity $S \in (0, 1]$ called *stealth* is assumed to be known. This is the probability that cyber-weapon continues to be useful (i.e., function) given that it has been deployed. The related quantity is *persistence* $P \in (0, 1]$ which is the the probability that a cyber-weapon continues to be useful given that it is not deployed. In essence, S captures the probability that an adversary will discover (and disable) a deployed cyber-weapon while P captures the probability that a non-deployed cyber-weapon will continue to be useful (i.e., that vulnerabilities it employs will not be discovered and patched). While difficult to measure there is sufficient historical information to estimate values for S and P.

Axelrod and Iliev also assume a random variable s (with range in $\mathbb{R}$) called the *stakes* which are vaguely defined as the importance of the cyber-attack to the attacker and assume that a threshold for this random variable is used to govern the attack. A gain function $G : \mathbb{R} \to \mathbb{R}$ is applied to the threshold T, which is to be determined. Axelrod and Iliev then state the discounted value of the cyber-weapon assuming a discounting (interest) rate $w \in (0, 1]$. In this model, they assume two time periods: the present and the future. In the present we know the stakes, and if the stakes are higher than the threshold we deploy the weapon and get the value $G(T) + wSV$. If the stakes are lower than the threshold, we do not deploy the weapon and only get the future value wPV. Thus, they define the total value as a function of T as:

$$V = \Pr(s > T)\,(G(T) + wSV) + (1 - \Pr(s > T))\,wPV \quad (1)$$

This recurrence equation can then be solved (algebraically) for V to determine V as a function of T assuming that the probability distribution of the stakes is known and $G(T)$ is also known. The *optimal timing* in their paper is actually the determination of an optimal threshold T_{opt}.

There are a few simplifications–and a few complications–in this model that make it impractical and unrealistic. First off, stakes are too poorly defined to be of

any use and in a highly polarized environment (common in political decision environments) every situation is considered to be *high stakes*. Moreover, it seems that gain is mixed with stakes, where presumably the higher the stakes the higher the gain, so these two factors could be consolidated into one estimation. In this model the stakes are considered to be a random variable which is independent of time. Yet, the authors attempt to couple optimal *threshold* with optimal *timing*, however the two should not be coupled if stakes are time-independent. In the real world, the stakes of tomorrow should be a function of the present stakes and thus dependent on time. Furthermore, the model's gain function does not seem to take into account the losses that can occur after a cyber-weapon has been deployed for an extended period of time (e.g., the German discovery of the bugging of Angela Merkel's phone leading to diplomatic harm). Instead, they assume that the value of the weapon is fixed. Consequently, this model may encourage the use of cyber-weapons early and often.

Ideally, we want a model which tells us *when* to deploy our weapon, instead of giving us an immeasurable quantity (threshold) on which to base our deployment. We propose a different model which reduces the use of unknown elements, and creates a more realistic and practical method for determining optimal timing. As before, let P be the persistence of a cyber-weapon and let S be its stealth. We dismiss the stakes random variable and simply consider a a gain function of time $G(t)$, which stakes is consolidated into, and loss variable L. In the sequel, we will consider cases were these are not random, but governed by known functions as well random walks. We simplify the "value" of the cyber weapon to be its gains minus its losses. A cyber-weapon deployed at time τ (the value we are interested in determining) is then given by:

$$V(\tau) = P^\tau w^\tau G(\tau) + \sum_{t>\tau} w^t \left(\mathbb{E}[G(t)]S^{t-\tau} + \mathbb{E}[L(t)](1-S^{t-\tau})\right) \quad (2)$$

This expression correctly takes into account loss as a result of a failure of stealth and requires the estimation of four parameters:

1. The persistence P,
2. the stealth S,
3. the gain function (or stochastic process) $G(t)$,
4. the loss function (or stochastic process) $L(t)$

Gain and loss functions can be modeled through ordinal values as was done in the game theoretic model of the Battle of Avranches [15] or through consensus estimates among decision makers and stake-holders themselves [16]. The goal for a decision maker is to determine, given these parameters, the optimal time τ to release a cyber-weapon.

III DECAYING OR CONSTANT GAINS AND LOSSES

Consider the case when:

$$G(t) = \beta^t G$$
$$L(t) = \gamma^t L$$

for fixed values $G \geq 0$ and $L \leq 0$. Then Equation 2 becomes:

$$V(\tau) = P^\tau w^\tau G(\tau) + \sum_{t>\tau} w^t \left(G\beta^{t-\tau}S^{t-\tau} + G\gamma^{t-\tau}(1-S^{t-\tau})\right) \quad (3)$$

In the case when γ or β are 1, then this is a constant gain or loss scenario. After an algebraic analysis, we can re-write Expression 3 as:

$$V(\tau) = (Pw)^\tau G + w^{\tau+1}\left[\frac{L}{1-w\gamma} + \frac{wS\beta G}{1-wS\beta} - \frac{wS\gamma L}{1-wS\gamma}\right] \quad (4)$$

Let:

$$p = Pw$$
$$R(G,L) = \frac{L}{1-w\gamma} + \frac{wS\beta G}{1-wS\beta} - \frac{wS\gamma L}{1-wS\gamma}$$

Then Equation 4 can be written as:

$$V(\tau) = Gp^\tau + R(G,L)w^{\tau+1} \quad (5)$$

This function has an extremum at:

$$\tau^* = \frac{\log(w) - \log\left(-\frac{G\log(p)}{R\log(w)}\right)}{\log(p) - \log(w)} \quad (6)$$

which may or may not be exogenous or positive depending on the sign of the numerator. To see this note, that $p < w$ (by assumption) and therefore the denominator is always negative. Moreover, the term:

$$\log\left(-\frac{G\log(p)}{R\log(w)}\right) \quad (7)$$

is real only when $R < 0$, since $G > 0$ by assumption. Thus:

$$\tau^* > 0 \iff \log(w) < \log\left(-\frac{G\log(p)}{R\log(w)}\right) \iff$$
$$w < -\frac{G\log(p)}{R\log(w)} \iff -\frac{Rw}{G} < \frac{\log(p)}{\log(w)}$$

because $R < 0$ by assumption. Thus we have proved:

Proposition 1. *The value function $V(\tau)$ has a real positive extremum if and only if $R < 0$ and :*

$$-\frac{R}{G} < \frac{\log(p)}{w\log(w)} \tag{8}$$

We can now characterize the nature of this extremum. Note that $V'(0)$ is:

$$G\log(p) + Rw\log(w) \tag{9}$$

Thus:

$$V'(0) > 0 \iff G\log(p) + Rw\log(w) > 0 \iff$$
$$-\frac{R}{G} > \frac{\log(p)}{w\log(w)}$$

Combining this with Proposition 1 we see:

Proposition 2. *Any real, positive local extremum of $V(\tau)$ is a minimum.*

Finally, note that:

$$V(0) = G + Rw \tag{10}$$
$$\lim_{\tau\to\infty} V(\tau) = 0 \tag{11}$$

Thus, we may conclude the following about the model under the given assumptions:

Proposition 3. *If $G + Rw > 0$, then $V(\tau)$ is maximized at $\tau = 0$ and the cyber-weapon should be deployed at $\tau = 0$. Otherwise, the cyber-weapon should not be deployed.*

IV RANDOM WALK GAINS AND LOSSES

A more realistic model for gain is a stochastic process such as a random walk. In this case, $G(t)$ depends only on the gains at the previous time step, and can either increase or decrease from $G(t-1)$. If we consider a scenario playing out day-by-day, each day the situation could be slightly mitigated, or slightly worsened. This is accurately modeled by a random walk. Depending on the situation, we could alter the parameters of the random walk and, for instance, place a higher probability on the situation getting worse than getting better. For simplicity, in this section we leave the loss, L, constant.

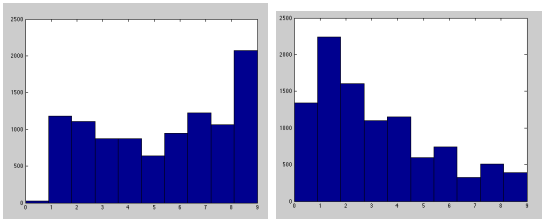
The main difference with this model is that, after the time of deployment, the future gains are unknown. Thus, at the time of deployment τ, a known gain $G(\tau)$ is collected, but for $t > \tau$ the gains are unknown, so we must explicitly consider $\mathbb{E}[G(t)]$. The value of deploying the weapon at time τ continues to be given by Equation 2, but modified to consider our constant loss function:

$$V(\tau) = P^\tau w^\tau G(\tau) + \sum_{t>\tau} w^t \left(\mathbb{E}[G(t)]S^{t-\tau} + L(1 - S^{t-\tau})\right) \tag{12}$$

For simplicity, we will only consider examples where $G(t)$ is a symmetric random walk on $\mathbb{R}$ with step size s, meaning that $\Pr(G(t) = G(t-1) + s) = \frac{1}{2}$ and $\Pr(G(t) = G(t-1) - s) = \frac{1}{2}$. Since the walk is symmetric, $\mathbb{E}[G(t)] = G(\tau)$ for all $t > \tau$.

In order to numerically estimate the optimal deployment time, we simulate this random walk 10,000 times with a given set of parameters and step sizes, and determine which deployment time is optimal for each iteration. For each iteration, we start at $G(0)$ and calculate $V(0)$. The walk then takes one step which randomly increases or decreases G by s, and we calculate $V(1)$ based on $G(1)$, where $G(1)$ is either $G(0) - s$ or $G(0) + s$. We run this over 10 time steps, and then chose the time that yielded that highest value as our optimal time of deployment. As shown in the figures below, we constructed a histogram of the number of instances that each t was optimal. Over the 10,000 trials, this gives us an approximate percentage of the time that a specific τ will be optimal for a given set of parameters and step size. In terms of gains, since the value function depends only on $G(\tau)$ and $\mathbb{E}[G(t)]$, it was surprising to find that the step size of the random walk dramatically alters the expected optimal time of deployment. We conducted experimental trials with two different step sizes (5 and 50), holding all other parameters constant at $P = 0.8$, $S = 0.2$, $w = 0.9$, and $L = -1$. Over 10,000 trials, a histogram of the optimal deployment time is shown below for both walks, keeping all other variables constant.

In the first histogram, the random walk has a step size of 5, and we see that, typically, the optimal deploy-



(a) $s = 5$ (b) $s = 50$

Figure 1: Histogram of optimal weapon deployment time with the gains modeled as a random walk

ment is at the last time step. However, in the second histogram, when the random walk has a step size of 50, we see that the optimal deployment time is much sooner, usually around time $t = 1$. This suggests that the variability in the walk, not the expected value of the walk, is an important determination for optimal deployment time.

We explain this phenomenon as follows: suppose we are interested in the probability of time τ being the optimal deployment time, given that we know $G(\tau) = k$. Suppose that the parameters w, P, S, and L are fixed, and $G(t)$ is modeled by a simple symmetric random walk with step size s.

In order for τ to be the optimal deployment time, we need $V(\tau) > V(t)$ for all $t \neq \tau$. First consider all $t > \tau$. For each t we can compute $G_t^* = \max_G\{V(t) \mid V(t) \leq V(\tau)\}$. Then $M_t = \frac{G_t^*}{s}$ is the maximum number of positive steps a random walk starting at 0 could take by time t in order to preserve τ as the optimal deployment time [2]. Thus, the probability that τ is the optimal time of deployment given that we know $G(\tau) = k$ can be directly calculated by counting the number of walks that are less then M_t by time t, start at the origin, and go through the point (τ, k), as illustrated in Figure 2 below.

We can simplify the expression for $V(\tau)$ by substituting all parameters except for k:

$$V(\tau) = c_1 + c_2 k \tag{13}$$

where c_1 is the component of the value that does not depend on k (i.e., the part that depends only on the loss), so c_1 is negative. For all $t > \tau$, we can say that

$$V(t) = c_1' + c_2' G(t) \tag{14}$$

where $c_1 < c_1'$ because from the model it is clear that the earlier we deploy, the more losses we incur over

[2]We can easily consider cases where $G(0) \neq 0$ by shifting the walk

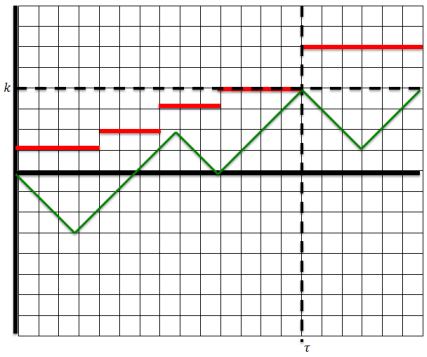


Figure 2: This figure illustrates the concept of M_t, shown in red. We are interested in the number of random walks that start at the origin, go through the points (τ, k), and stay below the red line. The green line indicates a random walk that follows these rules.

the total time span. We can calculate G_t^* by setting these two expressions equal to each other:

$$G_t^* = \frac{(c_1 - c_1') + c_2 k}{c_2'} \tag{15}$$

so

$$M_t = \frac{(c_1 - c_1') + c_2 k}{c_2' s} \tag{16}$$

Now suppose we are interested in learning what happens to M when we change s. Let s' be the new step size, and let all values with a prime be the corresponding values using s' instead of s. Then $k' = ks'/s$. Let $a = s/s'$. Then we obtain the following expression for M_t':

$$M_t' = \frac{a(c_1 - c_1') + c_2 k}{c_2' s} \tag{17}$$

Since $(c_1 - c_1')$ is negative, when $a > 1$, $M_t' < M_t$, meaning that:

$$\Pr(V(\tau) > V(t) | t > \tau) > \Pr(V'(\tau) > V'(t) | t > \tau). \tag{18}$$

So when s' is smaller than s, there is a smaller chance that τ is the optimal deployment time for all $t > \tau$.

Now we consider $t < \tau$. In order to calculate the maximum number of positive steps that $G(t)$ could take by time t and still maintain τ as the optimal deployment time, we now take $M_t = \frac{G_t^*}{s}$. The probability that $V(t) > V(\tau)$ for all $t < \tau$ is simply the proportion of random walks that begin at the origin, stay below M_t at time t, and end up at $\frac{k}{s}$ compared to the total number of random walks starting at the origin and ending at $\frac{k}{s}$ at time τ. Now we refer back

to Equation 17 to see what happens when we consider a step size s' instead of s. Since $t < \tau$, $c_1 - c_1'$ is now positive, so when $a > 1$ we have $M_t' > M_t$, meaning that

$$\Pr(V(\tau) > V(t) | t < \tau) < \Pr(V'(\tau) > V'(t) | t < \tau). \tag{19}$$

A diagram depicting these results is below.

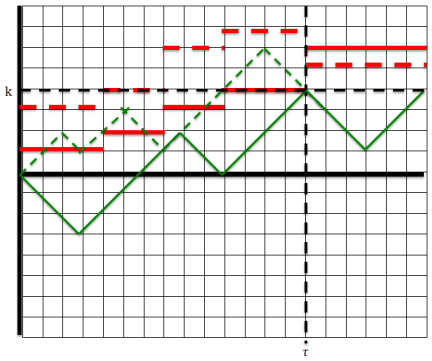


Figure 3: The red lines indicate G_t, the boundary that the walk must remain below. The dashed red lines shows G_t when the step size is 5, and the solid red lines shows G_t when the step size is 50. The green dashed and solid line, respectively indicate possible random walks that start at the origin, stay below the dashed and solid red lines, respectively, and go through the point (τ, k).

Qualitatively, these results indicate that early deployment times are favored when s is large and later deployment times are favored when s is small, which is what we observed in the example at the beginning of this section.

V COMPARISON TO REAL-WORLD EVENTS

Our model suggests alternative explanations for the decision of when to deploy a cyber weapon. In [9], Axelrod and Iliev consider a number of historical examples to validate their model, claiming that early deployment times are either indicative of very high stakes, high stealth, or low persistence. Using a random walk model for gains (which are analogous to high stakes, assuming that higher stakes yields higher gains), we find that high variability or uncertainty in future Gains can also lead to early deployment times, and that greater certainty in future Gains leads to later deployment times. Alternatively, using our constant/diminishing gains model, we see that early deployment is consistent with a perception of very low likelihood of loss or extremely large gains.

Note: this section simply re-analyzes scenarios provided in [9]. To our knowledge, all activities are alleged. This section is not meant to accuse or assert the veracity of any claim made in [9]; e.g., at no point in time has any official from the Chinese government substantiated the allocations of Chinese espionage discussed in the sequel. In fact, these allegations have been repeatedly denied.

1 STUXNET

First we look to the example of Stuxnet. According to Axelrod and Iliev's analysis of the situation, Stuxnet had poor Persistence and comparatively good Stealth. Furthermore, Axelrod and Iliev argue the stakes were high in the situation, suggesting a large gain. We infer that because the Stuxnet code escaped, there were significant losses to using the weapon. Applying this situation our model, we use the following parameters: $P = 0.2$, $S = 0.8$, $w = 0.9$, $L = -2$, $G(0) = 5$, $s = 1$. This means that Stuxnet had low Persistence, high Stealth, significant losses, high initial gains, and low variability in the future gains. Using our random walk model, we find that immediate deployment is always optimal. Moreover, using a constant gain / loss model (i.e., $\beta = \gamma = 1$) we see a similar result, with $\tau = 0$ being the optimal deployment time (i.e., deploy immediately). This is illustrated in Figure 4. Conversely, when the step sized is changed to $s = 5$, immediate deployment is is only optimal about 35% of the time, and almost every time step is optimal a significant portion of the time. Thus, it is far less clear when to deploy when there is more uncertainty in the gains (or stakes, in Axelrod's model). In general, we conclude the very intuitive result that weapons with low persistence, high stealth, significant losses, and high immediate gains should be deployed imme-

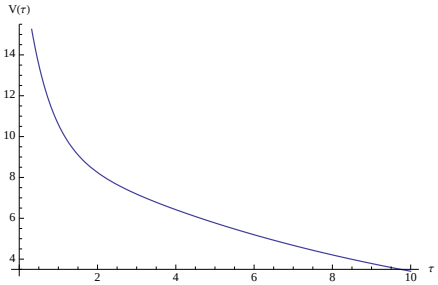


Figure 4: The computed $V(\tau)$ for a constant gain/loss model of StuxNet deployment.

diately *unless* there is very high uncertainty in future gains, in which case a later deployment time could be optimal.

2 IRANIAN ATTACK ON SAUDI ARAMCO

Compared to the Stuxnet example, Axelrod and Iliev cite this example as one in which the stealth of the attack was poor. Thus, we choose $S = 0.4$, and keep $P = 0.2, w = 0.9$, and $L = -2$. For the random walk model, if all parameters are held constant (using $s = 5$) and we vary $G(0)$, our model predicts that for $G(0) < 5.7$, the weapon should be deployed in a late time period, but if $G(0) > 5.7$, then the weapon should be deployed immediately. Since the Iranians did use their cyber weapons immediately, they must have perceived their gains to be very large. However, we could also consider how the variability in the gains could have affected the Iranians perception. Even with low initial gains, by increasing the step size we can achieve early deployment. and the Iranians believed that the gains were very volatile. This can be factored into our model by increasing the step size of our random walk. Thus, the Iranians could have either perceived extremely high gains, or a very uncertain future about the gains. The constant gain/loss model provides similar results with $G > 11.3$ resulting in immediate deployment and $G < 11.3$ resulting in a later deployment time.

3 EVERYDAY CHINESE CYBER ESPIONAGE

Axelrod and Iliev attempt to use their model to explain why the Chinese continually launch cyber attacks against the US, when they have only moderate Stealth and relatively low gains, instead of waiting until when the gains are higher. The possible explanations that are cited for this behavior are either that the Chinese believed their weapons to have low persistence, or they believed that their weapons would have high stealth against some targets because some outlier targets have been slow to detect them. We use our random walk model with moderately low current gains $G(0) = 5$, relatively low loss, $L = -1$, and moderate Stealth, $S = 0.5$. We vary the Persistence and the step size to search for possible explanations. With $P = 0.8$ and $s = 1$, our model predicts that the latest possible deployment time is optimal about 24% of the time, and immediate deployment is almost never optimal. When $P = 0.2$, the latest deployment time is optimal about 35% of the time, and immediate deployment is, again, almost never optimal. Thus, change in persistence does not seem to be the driving force behind early or late deployment time.

However, when step size is increased and $P = 0.2$ *or* $P = 0.8$, early deployment times become optimal. In conclusion, when gains are moderately low and have low uncertainty, our model indicates that even a drastic reduction in P would not account for early deployment. With low gains, the uncertainty in future gains is a potential driving force behind the deployment time. (If the cyber weapons did in fact have high Stealth against some targets, this could also be a driving force.)

Interestingly, this is a case where the constant gain/loss model differs from the random walk model. For all values of persistence, with $S = 0.5$, $G = 5$ and $L = -1$ and $w = 0.9$, we conclude that immediate deployment is optimal. In this case, the value of L is the driving factor in the decision.

4 PREMATURE CHINESE USE OF A HIGH-PERSISTENCE, LOW-STEALTH RESOURCE

In this section, Axelrod and Iliev use the example of the Chinese halt of its rare-earth exports pressure to provide strong economic pressure against Japan. In summary, in conflict with Japan, China cut off its exports of rare earth materials. China controlled 97% of the market, and Japan imported half of that. This economic warfare had high persistence and very low stealth. In these situations, there should be a very high threshold for use, and it is difficult to justify China's immediate use of economic power when the future stakes would probably have been higher. In this case, since it was predicted that future stakes would be higher, we would model this with an asymmetric random walk. If we set current gains at $G(0) = 5$, then a realistic random walk might be $Pr(G(t+1) = G(t) + 5) = 0.8$, and $Pr(G(t+1) = G(t) - 5) = 0.2$ Using the parameters $P = 0.8, S = 0.1$, and $L = -1$, our model predicts that the latest deployment time is optimal about half of the time. Thus, we agree with Axelrod and Iliev that the Chinese desire to immediately economically harm the Japanese overwhelmed their rational decision making. They could have gained more by waiting to deploy at a later time. This case is particularly interesting because it cannot be modeled by the constant/diminishing gain and loss model and requires a model consistent with

gains following a random walk.

VI CONCLUSIONS AND FUTURE DIRECTIONS

Inspired by the work of Axelrod and Iliev [9], we have proposed a stochastic model of the value of deploying a cyber-weapon at a specific time. Our model extends the work in [9] by explicitly incorporating a stochastic time-varying gain function and (as needed) a stochastic time varying loss function. When the gain/loss functions are geometrically decreasing, we prove a simple rule of thumb on whether a cyber-weapon should be deployed. When the gains are given by a random walk, we illustrate cases where early and later deployments are probabilistically optimal.

In future work, we hope to consider more complex and realistic gain/loss functions and to develop methods for estimating the parameters P and S. Additionally, this model is qualitatively similar to some models from mathematical finance. It would be intriguing to evaluate modifications to these models to determine whether or not results from this field could be applied to the problem of cyber-weapons deployment. Finally, we have only considered one side of the interaction. Future work should consider more game-theoretic models of cyber-weapons release.

References

[1] J. Lewis, "Assessing the risks of cyber terrorism, cyber war and other cyber threats," *United States Center for Strategic and International Studies*, 2002.

[2] T. Gjelten, "Cyberattacks, terrorism top u.s. security threat report," *All Things Considered, NPR*, March 12 2013.

[3] J. Clapper, "Statement for the record: Worldwide threat assessment of the us intelligence community," US Senate Select Committee on Intelligence, Washington DC, 2013.

[4] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, 2013.

[5] M. J. Gross, "A declaration of cyber-war," *Vanity Fair*, 2011.

[6] L. Milevski, "Stuxnet and strategy: A special operation in cyberspace," *Joint Force Quarterly*, vol. 63, October 2011.

[7] N. C. Rowe, "Ethics of cyberwar attacks," in *Cyber War and Cyber Terrorism*. The Idea Group, 2007.

[8] P. Oltermann, "German mps complain about nsa silence on angela merkel hacking," *The Guardian*, November 18 2013.

[9] R. Axelrod and R. Iliev, "Timing of cyber conflict," *Proceedings of the National Academy of Science*, no. 1322638111, 2013.

[10] R. K. Ahuja, A. Kumar, K. C. Jha, and J. B. Orlin, "Exact and heuristic algorithms for the weapon-target assignment problem," *Operations Research*, vol. 55, no. 6, pp. 1136–1146, 2007. [Online]. Available: http://pubsonline.informs.org/doi/abs/10.1287/opre.1070.0440

[11] R. Laraki, E. Solan, and N. Vieille, "Continuous-time games of timing," *Journal of Economic Theory*, vol. 120, no. 2, pp. 206 – 238, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0022053104000493

[12] K. Hendricks, A. Weiss, and C. Wilson, "The war of attrition in continuous time with complete information," *Int. Econ. Review*, vol. 29, pp. 633–680, 1988.

[13] S. Karlin, "Mathematical methods and theory in games," in *Programming and Economics*. Addison-Wesley, 1958, vol. 2.

[14] T. Radzik and T. Raghavan, "Duels," in *Handbook of Game Theory with Economic Applications*. North Holland, 1994, pp. 761–768.

[15] S. J. Brams, *Game Theory and Politics*. Dover Press, 2004.

[16] S. Weinberger, "Intelligence agencies turn to crowdsourcing," *BBC Code Red*, October 10 2012.