Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

The Evolution of Network Based Cybersecurity Norms: An Analytical Narrative

Atin Basuchoudhary

Virginia Military Institute

Nazli Choucri

Massachusetts Institute of Technology

August 13, 2014

This material is based on work supported by the U.S. Office of Naval Research, Grant No. N00014-09-1-0597. Any opinions, findings, conclusions or recommendations therein are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

THE EVOLUTION OF NETWORK BASED CYBERSECURITY NORMS: An Analytical Narrative

Atin Basuchoudhary
Virginia Military Institute
Email:basuchoudharya@vmi.edu
Phone: 540 464 7450

Nazli Choucri
Massachusetts Institute of Technology
Email: nchoucri@mit.edu
Phone: 617-253-3119

Abstract

We examine coordination dilemmas in cybersecurity policy by using an already developed evolutionary game theoretical model [2]. We suggest that norms to encourage network based security systems may not evolve independently of international governance systems. In fact, certain kinds of state action may actually further discourage the evolution of such norms. This paper therefore suggests that specific system-wide cybersecurity systems will be more effective than network-specific security. We build on established analytical frameworks to develop a cumulative understanding of the dynamics at hand. This would allow us, in due course, to extend the contributions of evolutionary game theory to cybersecurity problems.

1. Introduction.

The emergence of cyberspace in the latter half of the twentieth century has proven to be one of the greatest challenges to national security in the first part of the twenty first century. State and non-state actors alike are mobilizing to find ways to manage this unexpected "byproduct" of a major technological innovation. This byproduct has generated large-scale disturbances in traditional modes of international relations, far more pervasive than that of the well-known growth of globalized interdependence and its rapid expansion of scale and scope. Indeed cyberspace is shaping the process of globalization itself.

At this writing, we observe an ever-increasing politicization of cyberspace, and notable realignment of international politics. Almost overnight, cyberspace had shifted from the safe domain of "low politics" to the volatile arena of "high politics" [4]. All of this is created by, and in turn reinforces, complex interconnections that make it near-impossible for individual actors, private or public, to chart autonomous cyber policies and expect any success.

Given that the international system remains "anarchic" in theory and to some notable extent in practice, the very reality of *entanglement* is a definitional feature of both the international system and the cyber domain. This is a parametric condition that cannot simply be assumed away. Thus, unless a network -- with its, actors, and interests -- is highly segregated from broader connectivity, the very reality around us makes autonomous action nearly impossible and inevitably reinforces demand for coordination in policies, postures, and operations

Policy options are many, but the constraints in action are powerful. For example all actors, traditional and cyber centered, state and non-state (including corporations, NGO's and the like) can chose to cooperate, or not. They can chose to participate in providing security in an interconnected space, or not to do so. Nevertheless, they are embedded in intricate networks. Connectivity, *per se*, has not only grown over time, but more importantly, it is has become a critical factor that shapes the parameters of interaction.

1.1 Purpose.

This paper is in the form of analytical narrative. We provide some analytical rigor to arguments and issues that are usually framed in strictly normative or discursive terms. We seek to capture the characteristic features of alternative cultures that shape strategic postures toward cyber security. For this purpose, we draw on a dynamic evolutionary

IEEE IRI 2014, August 13-15, 2014, San Francisco, California, USA
978-1-4799-5880-1/14/$31.00 ©2014 IEEE

game theoretical model developed to analyze interactions among different actors with different cultures and strategies [2] to illustrate that coordinated governance mechanisms face some headwinds if they are to emerge organically -- even though the gains from such coordination are explicitly higher than in localized security systems. In addition, we assume that nothing stands still. Therefore, change, *per se*, is another critical factor shaping prevailing conditions. By building on analytical frameworks already developed and reviewed, we also seek to develop some cumulative understanding of the dynamics at hand. This would allow us, in due course, to extend the contributions of evolutionary game theory to cyber security problems.

1.2 Overview.

Almost all known networks develop synergy of their own [3]. These can have a direct implication for global well-being.[1] This synergy can support or threaten the global order. Nevertheless, threats to realizing supportive-synergy toward global cohesion abound as a result of conflicts that encompass the architecture of cyberspace [9], governance [11], a desire for political control [6], and personal advantage [7]. These threats therefore challenge prevailing modes of governance at all levels of analysis [4].

Thus, the supportive synergy of productive or system-supporting actors in cyberspace stand in sharp contrast to predatory or system-undermining actors driven by pursuit of private benefits unconstrained by any sense of public responsibility. On an observational basis alone, it is clear that the current situation creates pressures for various actors in various networks to protect themselves from predators by "closing themselves off"; i.e. by creating protective mechanisms. In so doing, however, they will reduce their exposure to the synergistic gains from the utilization of cyberspace.

The above can be framed in terms of two contending cultures pursuing distinctive strategies for enhancing cyber security. One strategy is *system-wide security*, based on coordinated governance and anchored in principles, structures, and processes that retains and protects the synergistic cyberspace for all. The other strategy is *segmented security* based on enhancing local network security which concentrates on self-security and avoids coordination, but by necessity carries all the costs of security localization, and forgoes all benefits accrued due to coordination.

This brief description, notwithstanding, it is clear that these two very different strategies signal powerful differences in cultures – all with respect to normative, behavioral, and strategic preferences and policy manifestations. We use the term "culture" here to refer to the dominant and overarching world-view that defines the beliefs, forms the preferences, and shapes propensities for actions and reactions. The differences between the two cultures depicted here capture some major dilemmas facing users of the Internet, as well as all providers of facilities and functionalities.

Most important of all: None of this is static. Change and transformation are fundamental features of social interactions, in all contexts, and at all levels of analysis. Accordingly, we cannot overlook the critical fact of change. Accordingly, drawing on the mathematics of biological evolutionary theory, we can also model cultural evolution [12]. In this paper, we seek to capture both the cultural and the dynamic elements that drive cybersecurity policy informed by an already developed nature-based evolutionary model [2].

We proceed as follows: In Section 2 we provide a theoretical exposition of initial model that we frame in this paper as a tradeoff between the global governance of cybersecurity and local, private security system. Section 3 presents and examines the evolution of cybersecurity norms. Section 4 highlights some implications of this inquiry and concludes.

[1] Reducing barriers to cyber access and increased sustainability increases this synergy [4, Fig 9.1, p. 207]

2. Theory – Culture, Coordination, and Change.

2.1 The Narrative Form.

This theory section restates the original model of rebel coordination developed in Basuchoudhary and Razzolini [2] to cybersecurity as a coordination dilemma, that is, a coordination problem between cultures with different approaches to implementing cybersecurity norms.

User Cultures: We begin with a population of computer users. There are three prevailing cultures dominated by distinct behavioral norms among these users – Always Cooperate (C), Always Defect (D), and Tit For Tat (TFT). We should note here that TFT represents a culture where defectors are punished in the future if they do not cooperate. Moreover, experimental evidence suggests that these are the most common strategies in one class of coordination games – the prisoner's dilemma [5]. People conform to cultural norms.

Bounded Rationality: However, people also learn about the benefits of belonging to another culture with some probability. They then switch to the other culture if it provides a higher benefit than their own. Thus, people from these different cultures --and underlying norms -- interact with each other. However, unlike in traditional game theoretic models people here have only "limited and localized knowledge concerning the system as a whole;" i.e. they are boundedly rational [8, p. 273].

We suggest this is a more realistic assumption than the hyper-rational, fully, if imperfectly, informed agents in the traditional coordination games. In this sense, our modeling assumption of bounded rationality is more plausible than classical game theoretic coordination games that also potentially capture the synergistic coordination versus defection trade-off in the politics of cybersecurity.

Coordination & Social Benefits: In this model, users in the Always Cooperate culture incorporate security systems that cover computer networks i.e. cyber security is coordinated though some global governance mechanism. Users from the Always Defect culture, on the other hand, secure their own computers and do not coordinate anything. Users from the TFT culture cover networks only if matched with the TFT or Cooperate cultures – otherwise they protect only their own computers.

The proportion of Always Cooperators in the population of users is p_c. The proportion of TFT is p_T. Therefore the proportion of Defectors is $1- p_T - p_c$. Table 1 represents the relative fitness of a particular culture in the evolutionary stage game. Cultures with an above average fitness will propagate through the population as a replicator dynamic [10]. The fitness of a particular strategy, however, depends on certain parameters. Let e be the net benefit from coordinating cyber security on the network.

We assume that the highest societal net benefit, e, comes from coordinating cyber security on the network. This assumption is grounded in the logic of the global networks. Also reasonable is the derivative view that if Cooperators can coordinate they divide the benefits equally. However, if a Cooperator and a Defector interact then the Cooperator bears the cost of implementing network cyber security. They also get a benefit from the network security but the cost of implementation reduces the net benefit – we normalize this net benefit to 0 for mathematical simplicity.

The Defector gets the benefit from the externalities created by implementing a network security system but does not bear the cost of implementation. However, the defector does not get the full benefit from the networked cyber security system either. Rather, the defector user gets some fraction α of the total security from a network based security system – thus garnering the Defector a payoff of αe. If a Defector interacts with another Defector then they are not nearly as safe as when there is a network security system since they each have their own security system that may not be safe from a diffuse hacker population. Moreover, disparate security systems may make it harder for computers to connect with each other.

Thus, each gets a payoff of $\alpha e/2$ which is by definition less than αe. Note that as α rises the relative fitness of the Defector rises as well. We assume that α tracks the ability of some institution to enforce a network based security system because such an institution, by definition would reduce the incentive to defect. Further, α tracks the returns to coordination. We get increasing returns to coordination for any $\alpha < 0.5$ and constant returns to coordination for any $\alpha > 0.5$. We ignore the case of decreasing returns to coordination since we start with the assumption that coordination of network security is synergistic.[2]

Interactions: Each network culture interacts with itself and other repeatedly. δ discounts the net

[2] See Anderton and Carter [1, p. 142-146] for a detailed example of how stag hunts and prisoner's dilemmas. respectively represent increasing and constant returns to coordination given that coordination is costly.

gains from future interactions. Thus, δ is a measure of "patience." A person with higher δ thinks the future is more valuable than a person with a lower δ. In other words, people with a higher δ are more willing to wait for the future, i.e. they are more patient. This gives us the evolutionary stage game below. This notion of patience is also a proxy for the reality of temporality and the role of "time".

2.2 The Analytical System.

Table 1 represents the evolutionary stage game. Thus, it pulls the pieces together and presents the entire logic.

Table 1. The Evolutionary Stage Game.

	Always Cooperate	**Always Defect**	**TFT**
Always Cooperate	$\frac{e}{2(1-\delta)}, \frac{e}{2(1-\delta)}$	$0, \frac{\alpha e}{(1-\delta)}$	$\frac{e}{2(1-\delta)}, \frac{e}{2(1-\delta)}$
Always Defect	$\frac{\alpha e}{(1-\delta)}, 0$	$\frac{\alpha e}{2(1-\delta)}, \frac{\alpha e}{2(1-\delta)}$	$\alpha e + \delta\alpha e/(2(1-\delta)),$ $\delta\alpha e/(2(1-\delta))$
TFT	$e/(2(1-\delta)),$ $e/(2(1-\delta))$	$\delta\alpha e/(2(1-\delta)), \alpha e + \delta\alpha e/(2(1-\delta))$	$\frac{e}{2(1-\delta)}, \frac{e}{2(1-\delta)}$

The expected payoff from Cooperation is:

$$E\pi_C = p_C\left(\frac{e}{2(1-\delta)}\right) + p_D 0 + p_T\left(\frac{e}{2(1-\delta)}\right) \quad (1)$$

The expected payoff from Defecting is:

$$E\pi_D = p_C\left(\frac{\alpha e}{(1-\delta)}\right) + p_D\left(\frac{\alpha e}{2(1-\delta)}\right) + p_T\left(\alpha e + \frac{\delta\alpha e}{2(1-\delta)}\right). \quad (2)$$

The expected payoff from TFT is:

$$E\pi_{TFT} = p_C\left(\frac{e}{2(1-\delta)}\right) + p_D\left(\frac{\delta\alpha e}{2(1-\delta)}\right) + p_T\left(\frac{e}{2(1-\delta)}\right). \quad (3)$$

Equations (1), (2), and (3) are the expected finesses for each culture. The replicator dynamic suggests that cultures that are fitter than average propagate through a population. Specifically, if an agent learns, with some probability, that her strategy has a lower expected payoff than another's, she will switch to the other strategy. Thus, we compare the average fitness of each culture to another to find the conditions for which one culture will be fitter than another. The strategy with the greatest average fitness of the three strategies will therefore propagate through the population. Below we show the conditions under which each of the three strategies we consider here are the fittest and therefore likely to propagate through the population.

TFT is fitter on average than Always Coop if:

$$\frac{e}{2(1-\delta)}[(p_C + p_T)(1-\delta\alpha) + \delta\alpha] > \left(\frac{e}{2(1-\delta)}\right)(p_C + p_T),$$

which simplifies to

$$p_C + p_T < 1. \quad (4)$$

TFT is better than Always Defect on average if

$$\frac{e}{2(1-\delta)}[(p_C + p_T)(1-\delta\alpha) + \delta\alpha] > \frac{\alpha e}{2(1-\delta)}[1 + p_C + p_T(1-\delta)],$$

which simplifies to

$$P_C > \frac{\alpha(1-\delta)}{(1-\alpha(1+\delta))} - \frac{(1-\alpha)P_T}{(1-\alpha(1+\delta))} \quad (5)$$

Always Defect is on average fitter than Always Coop if

$$p_C\left(\frac{\alpha e}{(1-\delta)}\right) + p_D\left(\frac{\alpha e}{2(1-\delta)}\right) + p_T\left(\alpha e + \frac{\delta\alpha e}{2(1-\delta)}\right) > p_C\left(\frac{e}{2(1-\delta)}\right) + p_D 0 + p_T\left(\frac{e}{2(1-\delta)}\right),$$

which simplifies to

$$P_C < \frac{\alpha}{1-\alpha} - P_T\frac{1-\alpha(1-\delta)}{(1-\alpha)}. \quad (6)$$

So far, we have presented the three network norm cultures or dominant modes of behavior, each in relation to the other, and we have built behavioral "rules" within an overarching context framed by the imperative of cooperation. This framing is identical to the first application of the generic model [2]. What follows is an application of this model to the cyber domain, followed by a discussion of its implications.

3. Evolution of Cyber Security Norms.

3.1 Attractors and Attractor Basins.

The model displayed above and its results [2] allow us to analyze whether networked cybersecurity norms can evolve or not. To do so, we first identify rest points and basins of attraction as a function of the incentive to defect (α) and patience (δ) for a general set of coordination games in the context of disorder (specifically rebellion).

Recall that we define the incentive to defect as a consequence of an *exogenous* overarching governance structure that enforces a network based security system. We make no assumption about the structure, process, or mechanism of governance, only about its existence and its effectiveness. We also make no assumption about membership type. We explore only the conditions under which the performance of such an organization can be effective.

Thus, a weak governance system would provide a higher incentive to defect, i.e. a higher α.

Recall, further, that rest points are population *mixes of strategies* that replicator dynamics do not disturb. Basins of attraction define population mixes that replicator dynamics move towards rest points. Such rest points are called attractors [10]. Here, we apply the results derived in Basuchoudhary and Razzolini [2] to analyze whether a culture that supports network-based security can be an attractor and the basin of attraction that would support such an attractor.

Then we show how these basins of attraction vary with the strength of a *governance system* that reduces the incentive to defect and the inherent patience of agents in the three cultures. This analysis therefore provides a methodology for understanding whether a cooperative networked culture can ever be part of a stable population mix or not -- as a function of international governance system and behavioral features of users.

Equations (4), (5), and (6) define basins of attraction for a particular culture in relation to another. Taken together they define basins of attraction for one of the three cultures we consider.

Figure 1 showcases a situation where the international governance system is strong, i.e., when $\alpha < 0.5$. Effectively, the evolutionary stage game is then a stag hunt. Stag hunts represent increasing returns to coordination when coordination is costly [1, p. 142-146]. Here, TFT is the fittest culture in regions A and B, while Defect is the fittest culture in region C. Thus, if the population mix of Cooperators and TFT (p_T, p_c) lie in region A or B, the entire population will over time learn the TFT culture while if the population mix of Cooperators and TFT lie in C then the entire population will learn the Always Defect culture.

Similarly, in Figure 2 we represent a situation where the international governance system is weak, i.e. when $\alpha > 0.5$. Effectively, the evolutionary stage game is then a prisoner's dilemma. Prisoner's dilemma's represent constant returns to coordination when coordination is costly [1, p.142-146]. Here, TFT is the fittest culture in regions E and F, while Defect is the fittest culture in region D. Thus, if the population mix of Cooperators and TFT (p_T, p_c) lie in region E or F, the entire population will, over time, learn the TFT culture while if the population mix of Cooperators and TFT lie in D then the entire population will learn the Always Defect culture. However, it turns out that the space enclosed in these regions changes as both α and δ change with implications for whether a cooperative networked cybersecurity system can ever be part of a stable population mix.

More specifically the Basuchoudhary and Razzolini [2] model prove three results that we will use to describe the cyber domain here. First, the Always Cooperate mode is never the fittest culture. Second, a TFT culture could enforce cooperation if the initial population proportion of the TFT culture is large enough. Third, the TFT culture is more likely to succeed as δ rises. Nevertheless, the success of the TFT culture is not guaranteed even when $\delta = 1$.

3.2 Cases and Constraints.

We should note that the evolutionary stage came in Table 1 is basically a stag hunt game or a prisoner's dilemma depending on whether $0 < \alpha < 0.5$ or $0.5 < \alpha < 1$ respectively. Basically, this means that there are increasing returns to coordination in the former case and decreasing returns to coordination in the latter given that coordination is costly [1]. Effectively, there is a greater synergy from productive actors in cyberspace in the former case than the latter. Recall that we characterize α as an exogenous factor, e.g. the ability of some international organization to enforce network security. Thus, a rising α tracks this organization's weakening ability to enforce a network based security which leads to less synergy from productive actors in cyberspace. Thus, applying Basuchoudhary and Razzolini [2] our discussion is constrained to two cases.

Case 1. $0 < \alpha < 0.5$. Figure 1 represents this case. Here, equations (4), (5), and (6) demarcate regions A, B, and C. Each region demarcates population distributions of people who belong to the Always Cooperate and Always Defect cultures (and therefore Always Defect). TFT is the fittest strategy in both region A and B. Thus if the distribution of the population among cultures falls in either region A or B over time more and more people will learn the TFT culture. In other words, regions A and B form the basin of attraction for the TFT culture. However, Always Defect is the fittest strategy in region C. Therefore, C is the basin of attraction for the Always Defect culture. Notice that as δ rises, the area C becomes a null set. In other words, Always Defect no longer has a basin of attraction and ceases to be an attractor. Thus, any realistic population distribution of Always Cooperate or TFT keeps TFT as the fittest strategy. Of course, the TFT strategy can sustain a cooperative culture. Thus, a network based security system is possible if there is a strong (low α) forward looking (high δ) international governance structure with an ability to retaliate against people or groups who defect from the system (TFT).

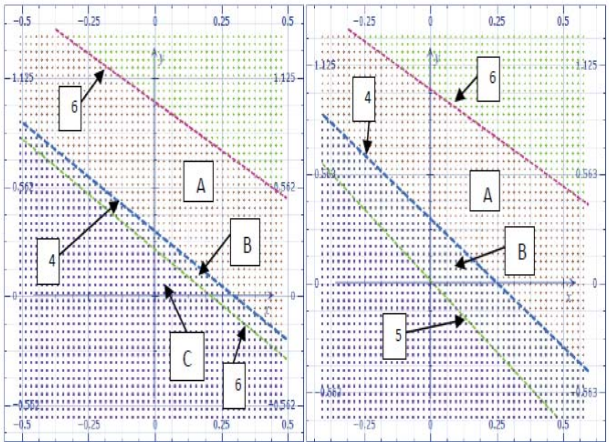
Case 2. $0.5 < \alpha < 1$. Figure 2 represents this case. Equations (4), (5), and (6) demarcate the

regions D, E, and F. Once again, these regions demarcate population distributions across Always Cooperate and TFT types (and therefore by default, Always Defect as well). In each region, a particular culture has the fittest strategy. Thus these regions, once again, are basins of attraction. Particularly, Always Defect is the fittest culture in D while TFT is the fittest strategy in regions E and F. Thus, D is a basin of attraction for Always Defect while E and F are basins of attraction for TFT. In other words, if the population distributions across the three cultures lies regions E and F people will learn to be TFT and this distribution will tilt towards the TFT strategy until everyone is part of the TFT culture. Similarly, a population distribution in D will incentivize the Always Defect culture and over time, people will learn to be Always Defect until everyone is part of the Always Defect culture.

As in the case above, Figure 2 shows that D becomes smaller as δ rises. Thus, even if international governance of network based security is weak (low α), as long as people are sufficiently forward looking (high δ), then a cooperatively networked security system can arise because the threat of defection remains a strong deterrent (TFT).

However, as Figure 3 shows, even with δ = 1, D, the basin of attraction for the Always Defect culture remains. Thus, while a rising δ increases the likelihood that a cooperative network based cybersecurity system may evolve, a weak governance structure can stymie this evolutionary process and lead to a fractured cybersecurity system centered on the individual rather than being system wide.

Figure 1.TFT becomes more likely to emerge as the fittest strategy as delta rises.[3]



[3] Fig 6a and 6b in [2]

Figure 2. TFT becomes more likely to emerge as the fittest strategy as delta rises.[4]

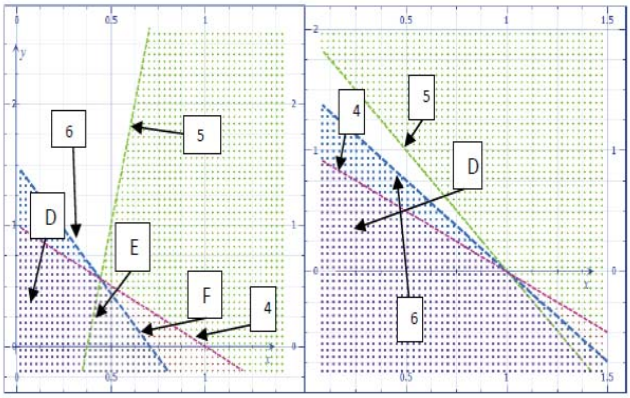
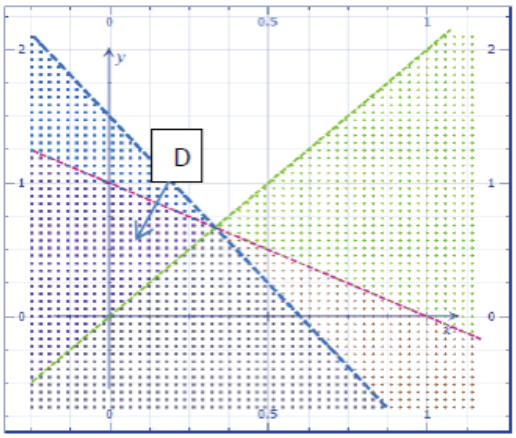


Figure 3. Always Defect may persist even when δ = 1[5]



4. Conclusion and Policy Implication.

In section 3 above we presented a game theoretical view of the evolution of a system-wide cooperative network, one that is based on shared cybersecurity norms. This view allows us to address some of the confounding factors central to current cybersecurity dilemmas, and to do so based on an internally consistent evolutionary game theoretical model [2].

4.1 Conclusion.

The analysis revealed that:

[4] Fig 7a and 7b in [2]

[5] Fig 7c in [2]

(a) a network based security system is possible if there is a strong forward looking international governance mechanism with an ability to enforce norms and to discipline or even to retaliate against any actors or entities who defect from the system,

(b) even if international governance of network based security is weak, as long as actors and entities, as well as their constituents are sufficiently patient, a cooperatively networked security system can develop with little credible threat of defection.

c) but patient agents alone are not sufficient for the evolution of a cooperatively networked security system as long as the governance structure remains weak and incentivizes the Always Defect culture, because the initial population mix plays a role in the direction of cultural evolution.

What might these results imply for policy?

4.2 Behavior Markers

First, we note that a strong international governance mechanism (high α) is no guarantee for implementing a networked cybersecurity system, even when it is possible to retaliate against defectors by denying them cybersecurity services. Thus, efforts to develop such security organization may fail if policy makers ignore behavioral markers – patience levels and temporal effects – of networked computer users. Indeed, there is a possibility that the very threat of retaliation may make agents impatient and reduce the effectiveness of governance.

Such endogenous changes in patience, and therefore desire to cooperate in implementing network-based cybersecurity systems, deserve further investigation.[6] Nevertheless, given a choice between hardening segmented individual systems that are part of a network or connecting to a networked-security system, the latter is only possible through some governance mechanism that allows TFT retaliation.

4.3 Enforcement Capacity.

Recall that the TFT strategy merely stands in for the ability to punish defectors. In other words, the ability to punish people -- actors or entities -- who defect from the networked-security system is quite important. This ability to punish requires authority and legitimacy. In today's world this means, among other things, an international legal frameworks enable by credible enforcement mechanisms.

Put differently, credible international policing or enforcing capabilities are essential for the overall system if system-networked cybersecurity is to evolve. This further suggests that since open security systems cannot legally enforce discipline mechanisms, they must incorporate some form of technological approach to punish defectors. In any case, none of that may be relevant if people are sufficiently impatient; i.e. δ is low. Once again, we return to the importance of patience and time.

4.4 Salience of Culture

In sum, this paper argues that ultimately the success or failure of implementing a network-wide security system depends on norms and behavioral characteristics of Internet users, rather than on technology *per se*. However, both technology and a legal structure may influence patience (i.e. time horizon) of users. For example, uncertainty about changes in governance mechanisms or uncertainty about the future of advances in Internet architecture may make agents impatient – and reduce their time horizon. This situation propels action. Thus, patience (δ) may be endogenous (Basuchoudhary, et al., 2010), in the sense that it both influences and is influenced by governance mechanisms (α) and by technology in ways that are not well understood. These relationships require further research.

4.5 Uncertainties and Change.

Last, this analytical narrative suggests that, as hitherto unconnected agents join the population of interconnected users, they change the proportions of the cultural types and the distribution of norms. These changes have implications for the likely emergence of global governance for a network-wide security system. For example, what happens if the population mix of internet users fall in region E in Figure 2? According to our argument, this population is well on its way to evolve a global governance mechanism. Then, as another population with a much larger number of agents who Always Defect joins the Internet the population mix may suddenly move to region D and destroy the evolutionary process towards a global governance structure.

Under these conditions, the very expansion of the Internet may carry the seeds of its destruction since without the networked-security system the synergistic feature of the Internet would be lost.

[6] For an initial foray in the theory of the evolution of patience, see Basuchoudhary, et al., (2010) and Basuchoudhary, et al., (2012).

Acknowledgement.

Basuchoudhary gratefully acknowledges research support provided by NSF grant BCS-904674. Any remaining errors are our own. We also acknowledge the DoD Minerva program's support.

Bibliography

[1] Anderton, C. H. & Carter, J. R., 2009. *Principle of Conflict Economics: A Primer For Social Scientists.* New York: Cambridge University Press.
[2] Basuchoudhary, A. & Razzolini, L., 2014. The Evolution of Revolution: Is Splintering Inevitable. *VMI Working Paper Series.*
[3] Brown, J. S. & Duguid, P., 2000. *The Social Life of Information.* Cambridge, MA: MIT Press.
[4] Choucri, N., 2012. *Cyberpolitics in International Relations.* Cambridge, MA: MIT Press.
[5] Dal-Bo, P. & Frechette, G. R., 2011. The Evolution of Cooperation in Infinitely Repeated Games: Experimental Evidence. *American Economic Review,* Volume 101, pp. 411-429.
[6] Deibert, R., Palfrey, J., Rohozinski, R. & Zittrain, J., 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace.* Cambridge, MA: MIT Press.
[7] Franklin, J., Perrig, A., Paxson, V. & Savage, S., 2007. *An Inquiry Into the Nature and Causes of the Wealth of Internet Miscreants.* s.l., Abstract from CCS: Proceedings of the 14th ACM Conference on Computer and Communications Security..
[8] Gintis, H., 2009. *Game Theory Evolving: A Problem Centered Introduction to Modeling Strategic Interaction..* 2 ed. Princeton(NJ): Princeton University Press.
[9] Goldsmith, J. & Wu, T., 2006. *Who Controls the Internet? Illusions of a Borderless World.* New York: Oxford University Press.
[10] Harrington, J., 2008. *Games, strategies, and decision making..* 1 ed. New York: Worth Publishers.
[11] Lessig, L., 1999. *Code and Other Laws of Cyberspace.* New York: Basic Books.
[12] McElreath, R. & Boyd, R., 2007. *Mathematical Models of Social Evolution: A Guide For the Perplexed.* Chicago: The University of Chicago Press.