DETERRENCE, INFLUENCE, CYBER ATTACK, AND CYBERWAR

PAUL K. DAVIS*

* Paul K. Davis is a senior principal researcher at the RAND Corporation and a professor of policy analysis in the Pardee RAND Graduate School. His early studies were in the hard sciences and he received a Ph.D. in theoretical chemical physics at M.I.T. After working on strategic technology and systems analysis at the Institute for Defense Analyses, he joined the U.S. government to work on strategic arms limitation, which included a period with the U.S. delegation in Geneva. He then joined the Defense Department where he worked initially on strategic nuclear programs before becoming a senior executive directing analysis of defense strategy and programs for the Persian Gulf (and, later, other regions worldwide). Dr. Davis then moved to the RAND Corporation in Santa Monica, where his research has been in strategic planning under deep uncertainty (primarily defense planning), decisionmaking theory, resource allocation, deterrence, and advanced methods of modeling and analysis. In recent years, his work has drawn on social science to inform analysis of counterterrorism and counterinsurgency. Dr. Davis teaches graduate courses in the Pardee RAND Graduate School where he emphasizes interdisciplinary work connecting analysis, the hard and soft sciences, planning, and modeling. Dr. Davis has served on numerous studies for the National Academy of Sciences, Defense Science Board, and other organizations. He reviews for or serves as associate editor on a number of academic journals.

I. Introduction

A. *Purpose*

Deterrence by itself is a fragile basis for strategic thinking. Thus, I start by placing deterrence within a broader framework of objectives and then discuss special features of the cyber attack challenge, distinguishing different classes and contexts of cyber threats.[1] I then use a simple model to speculate about whether deterrence can be a significant part of dealing with those different threats. The model allows for very different degrees of "rationality" on the part of whoever is to be deterred. My discussion ends with suggestions for policymakers and scholars. My conclusion is that hoping for deterrence with today's reality would be like grasping for straws. Deterrent measures should definitely be part of a larger strategy, but the focus should be elsewhere.

B. *Deterrence Is Merely an Element of Strategy*

Deterrence is a socially correct subject akin to "self-defense": The image is that an innocent subject fears attack and tries to deter the would-be aggressor by threatening punishment if attack occurs. Because of its favorable aura, people and organizations tend to appropriate the word "deter" for their own purposes. For example, it is sometimes claimed that *the* purpose of military forces is to deter aggression. This usage casts military planning in a favorable light but (1) obfuscates distinctions between protection and deterrence; (2) glosses over other objectives of military forces (such as actually fighting wars); and (3) confuses an element of strategy with the strategy itself. Referring loosely to deterrence can also inter-

---

1. Cyber attack is an attempt to damage, disrupt, or gain authorized access to a computer, computer system, or electronic communications network. I define cyberwar as an action by a nation-state or non-state group to penetrate a nation's computers or networks for the purposes of causing (significant) damage or disruption. This definition is close to that of Richard A. Clarke & Robert Knake, Cyber War: The Next Threat to National Security and What to Do about It 7 (2010). This does not include mischief, intelligence, crime, or "preparing the battlefield." Cyberwar will usually be part of larger conflict. Some authors use more inclusive definitions, while others think of cyberwar in Clausewitzian terms that require violence, an instrumental purpose, and a political nature. *See* Thomas Rid, *Cyber War Will Not Take Place*, 35 J. Strategic Stud. 5, 7–10 (2011).

fere with objective thinking, as when a side's "deterrent actions" and related posturing are seen by others as aggressive intimidation or bullying that require a response.

It is useful to elevate discussion to the level of objectives and to consider deterrence within that larger framework. Figure 1 is an attempt to do so with relatively generic objectives that apply to states, international businesses, and some other non-state actors (but not to revolutionary movements). The left-most objective is a kind of "stability" that allows for change without serious disruption, aggression, or coercion. It is about having a favorable normal environment. Moving rightward, another objective is to affect what transpires—perhaps with the benefit of military power or other types of influence, self-protection ability, or resilience. This objective is not necessarily high minded, since actors want to promote their interests even if they conflict with those of other actors. With stability as the norm and a reasonable ability to affect developments, things still go wrong and crises arise. Another objective is then crisis management. This has two aspects. On the one hand, certain instabilities are to be avoided, such as incentives for actors to make aggressive first moves. On the other hand, some actors want the ability to "dominate crisis" by having better options for escalation than do others. Finally, actors want to compete in the mostly stable environment—and to do so politically, economically, and in the realm of ideas and practices. As indicated in the gray cloud of Figure 1, an actor can use a variety of *influences* to achieve its objectives. Figure 2 shows a spectrum of influences, ranging from (on the left side) pleasant, nonviolent forms such as reducing fears or co-opting, to (on the right side) such uses of violence as punishing an actor now for past deeds so as to deter or preclude his future actions.[2] Clas-

2. This emphasis on influence rather than deterrence stems from earlier work on counterterrorism. *See* PAUL K. DAVIS & BRIAN MICHAEL JENKINS, DETERRENCE AND INFLUENCE IN COUNTERTERRORISM: A COMPONENT IN THE WAR ON AL QAEDA 11 (2002); Alexander L. George, *The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries*, *in* KNOW THY ENEMY: PROFILES OF ADVERSARY LEADERS AND THEIR STRATEGIC CULTURES 271, 272 (Barry R. Schneider & Jerrold M. Post eds., 2d ed. 2003); NATIONAL RESEARCH COUNCIL, U.S. AIR FORCE STRATEGIC DETERRENCE ANALYTIC CAPABILITIES: AN ASSESSMENT OF TOOLS, METHODS, AND APPROACHES FOR THE 21ST CENTURY SECURITY ENVIRONMENT (2014); *see also* Paul K. Davis, *Structuring Analysis to Support Future Nuclear Forces and Postures* (RAND Nat'l Def. Research Inst. Working Paper No. 878, 2011).

sic deterrence by threat of punishment is but one item in the spectrum.

For cyberspace specifically, major nations want stability, but they also want to use cyber attacks for intelligence and actions in crisis or conflict. If crisis occurs, they want to avoid unintended escalation—but to be better able to escalate than others. And, whatever the rules of the road, they want to be as effective as possible in cyberspace.

FIGURE 1. OBJECTIVES IN STRATEGIC PLANNING

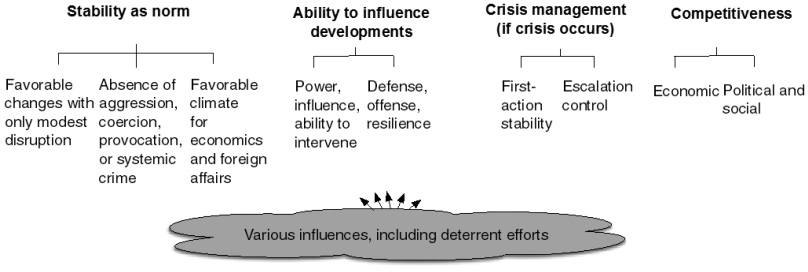
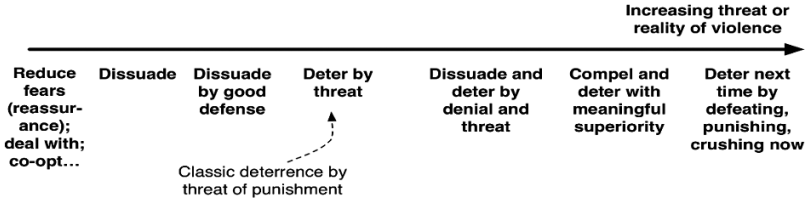


FIGURE 2. A SPECTRUM OF INFLUENCES



Another reason for seeing deterrence as merely one part of the picture is that, strategically, a *deterrent effort seldom succeeds by itself.* This is true even though the usual definition of classic deterrence is that "to deter" is *to convince an adversary not to take some action by threatening punishment if the action is taken.*[3] This definition misleads by treating the deterrent threat as "the" cause.[4] How often does a major actor not do something strictly because of threatened punishment? Even in the most

3. Thomas Schelling called deterrence "a threat intended to keep [the adversary] from doing something." THOMAS C. SCHELLING, ARMS AND INFLUENCE 69 (1966).

4. Similarly, it is sometimes said that cyber deterrence succeeds when an adversary decides not to act aggressively. Actually, the decision may have had nothing to do with the deterrent strategy.

famous alleged example of deterrence, the Cuban Missile Crisis, President Kennedy and Premier Nikita Khrushchev negotiated a bargain acceptable to both sides. Fear of nuclear war concentrated minds, but Kennedy secretly promised to pull missiles out of Turkey and, more important, not to invade Cuba. Without such a bargain, it is unclear what might have happened. The resolution of crisis also depended on the personal characteristics of the leaders involved. They rose above their advisors and saw each other as rational human politicians who cared deeply about their countries, not just as opponents in a power game.[5]

The notion that deterrent efforts stand alone is a bad idealization because it departs markedly from the usual reality of multiple interacting factors. Figure 3 is my effort to do better by imagining that our adversary is considering just two courses of action: the one we prefer (left) and the one we want to avoid (right).[6] In the simplest of decision models, the adversary compares the pros and cons of the two actions and chooses the one that seems better on balance. We can hope to affect his decisions with influences (items below the dotted line) by reinforcing the "pros" that he sees for the first option, by reducing the "cons" that he sees (perhaps by reassuring him that we have no bad intentions toward him), or by undercutting the pros that he sees for the second option. The latter might mean having defenses that would defeat attack, resilience that would make even a temporarily effective attack futile, or both. We might also elevate his recognition of the second option's cons, as by threatening punishment. We might

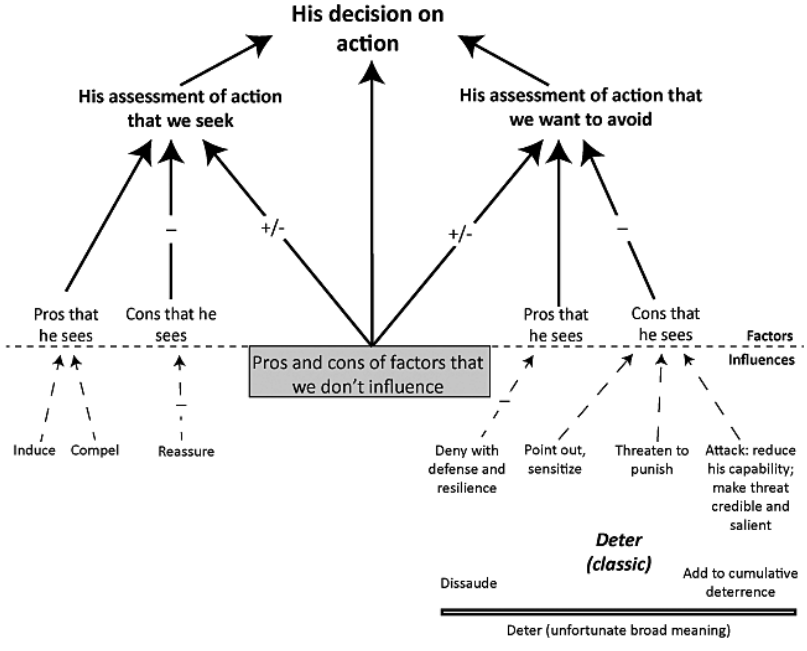
---

5. The world was far closer to the brink even than participants realized at the time. *See, e.g.*, MICHAEL DOBBS, ONE MINUTE TO MIDNIGHT (2008); A. A. FURSENKO & TIMOTHY J. NAFTALI, ONE HELL OF A GAMBLE: KHRUSHCHEV, CASTRO, AND KENNEDY, 1958-1964 (1st ed. 1997); JAMES A. NATHAN, THE CUBAN MISSILE CRISIS REVISITED (1992); Paul H. Nitze, *Reflections on the Cuban Missile Crisis*, COSMOS (1998), *available at* http://www.cosmos-club.org/journals/1998/nitze.html; *Interview With Robert McNamara: Episode 11 Vietnam*, THE NATIONAL SECURITY ARCHIVE (Dec. 6, 1998), *available at* http://www2.gwu.edu/~nsarchiv/coldwar/interviews/episode-11/mcnamara1.html.

6. In this influence diagram, if an arrow points from A to B, it means that more of A will tend to mean more or less of B, depending on whether the arrow's sign is positive (default), negative, or ambiguous (+/-). In some situations there may be no effect because, for example, other factors preclude any effect.

levy actual punishment now to sensitize him to what might follow, thereby re-establishing deterrence, or, using other terminology, improving "cumulative deterrence."[7]

FIGURE 3. FACTORS AFFECTING A DECISION



As shown in the grayed box, the adversary's decision is also subject to factors that we cannot easily influence, such as internal politics, nationalism, pride, and rationality. These will often be dominant, which is one reason that deterrence has often failed—even to the extent of the weak attacking the strong.[8]

As shown at the bottom of Figure 3, the word "deterrence" is often given a broad meaning that combines dissuasion, classic deterrence by threat of punishment, and cumula-

7. Increasing "salience" of threat goes beyond making the threat "credible," which to me justifies the concept of cumulative deterrence. *See, e.g.*, NATIONAL RESEARCH COUNCIL, *supra* note 2, ch. 2. R

8. *See generally* JOHN ARQUILLA, DUBIOUS BATTLES: AGGRESSION, DEFEAT, AND THE INTERNATIONAL SYSTEM (1992); BARRY WOLF, WHEN THE WEAK ATTACK THE STRONG: FAILURES OF DETERRENCE (1991).

tive deterrence. "Deterrence" is sometimes given even broader meanings that include offering reassurances and inducements on the one hand or trying to compel action on the other. Such indiscriminate usage undercuts discourse.[9] I reserve "deter" for the classic meaning that involves threat of punishment. I also refer to "dissuasion by denial," rather than "deterrence by denial," and define it as:

> dissuading an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action.[10]

This improves on the original concept of deterrence by denial by referring to what the adversary "sees," whether he regards that as credible, and whether he sees the potential gains as good enough by some criteria.[11] The word "potential" avoids assuming that the adversary bases his judgment on expected subjective utility as in rational-actor theory. The use of "dissuade" is consistent with its classic meaning of "persuade."[12]

Figure 3 says nothing about how the adversary combines considerations in choosing among options. The combining rules may be subtle and nonlinear. By and large, we are on stronger ground identifying the factors affecting decisions and the directionality of their influences, i.e., using qualitative models, than in purporting to predict the overall result.[13]

---

9. Organizations may be required to focus on deterrence, even if they know better. They may then finesse the limitations by effectively extending the definition. *See* U.S. STRATEGIC COMMAND, DETERRENCE OPERATIONS JOINT OPERATING CONCEPT 28–76 (version 2.0 2006). STRATCOM's responsibilities have been extended by Congress since the document cited was prepared.

10. Paul K. Davis, *Toward Theory for Dissuasion (or Deterrence) by Denial: Using Simple Cognitive Models of the Adversary to Inform Strategy* 2 (RAND, Working Paper No. WR-1027).

11. The original definition was due to Glenn H. Snyder, *Deterrence and Power*, 4 J. CONFLICT RESOL. 163, 163–78 (1960).

12. Some other authors treat denial more or less the same way as I have. *See, e.g.*, MARTIN C. LIBICKI, CRISIS AND ESCALATION IN CYBERSPACE 159 (2012); John Sawyer, *Dissuasion by Denial in Counterterrorism: Theoretical and Empirical Deficiencies*, *in* DETERRENCE BY DENIAL: THEORY, PRACTICE, AND EMPIRICISM (Andreas Wenger & Alex Wilner eds.) (forthcoming); Kenneth N. Waltz, *Nuclear Myths and Political Realities*, 84 AM. POL. SCI. REV. 731, 737 (1990).

13. *See* Paul K. Davis, *Representing Social Science Knowledge Analytically*, *in* SOCIAL SCIENCE FOR COUNTERTERRORISM: PUTTING THE PIECES TOGETHER 401 (Paul K. Davis & Kim Cragin eds., 2009); Paul K. Davis, *Specifying the Content*

However, it is arguably possible to do somewhat better by working with certain "fuzzy" kinds of mathematics that preserve and emphasize residual uncertainty, as illustrated in recent prototype research to understand public support for terrorism.[14]

Let us now turn from higher-level abstractions to more specific discussion about deterrence and influence with respect to cyber attack and cyberwar.

II. Deterrence and Cyberwar

A. *Selected Review of the Literature*

The challenges of cyberwar and netwar were discussed two decades ago in prescient work by John Arquilla and David Ronfeldt,[15] well before concepts such as network-centric operations were part of the mainstream and well before it was realized that small networked units can have disproportionately powerful effects and can even defeat large organizations such as states. The authors argued famously that "[i]t may take networks to counter networks. The future may belong to whoever masters the network form."[16] After a decade of wars with terrorist groups and insurgents rather than standing armies, the truth of their argument is rather clear.

Cyber deterrence has been discussed in a number of more recent papers. In an influential study, Martin Libicki concludes that cyber attack is more fundamentally different from earlier forms of conflict than had often been recognized.[17] Table 1 summarizes some of his conclusions and hard questions.

---

of Humble Social Science Models, *in* Proceedings of the 2009 Summer Computer Simulation (O. Balci et al. eds., 2009).

14. Paul K. Davis & Angela O'Mahony, A Computational Model of Public Support for Insurgency and Terrorism: A Prototype for More General Social-Science Modeling (2013).

15. John Arquilla & David Ronfeldt, *Cyberwar is Coming!*, 12 Comp. Strategy 141 (1993).

16. John Arquilla et al., *Networks, Netwar, and Information-Age Terrorism*, *in* Countering the New Terrorism 39, 82 (Ian O. Lesser et al. eds., 1998).

17. *See* Martin C. Libicki, Cyberdeterrence and Cyberwar xiii (2009).

TABLE 1. OBSERVATIONS AND ISSUES ABOUT CYBERWAR

Cyber has its own rules
Cyberwar is only possible because systems have flaws
Operational cyberwar has an important niche role, but only that
Strategic cyberwar is unlikely to be decisive
Cyber deterrence may not work as well as nuclear deterrence
Cyber deterrence raises difficult questions:
Will we know who did it?
Can retaliators hold assets at risk?
Can they do so repeatedly?
Can cyber attacks disarm cyber attackers?
Will third parties stay out of the way?
Might retaliation send the wrong message?
Can states set thresholds for response?
Can escalation be avoided?

Libicki sees cyber attacks as important, but largely as part of modern war. He and others such as Thomas Rid are skeptical about stand-alone strategic cyberwar because cyber attacks do not capture territory and are likely to have temporary and uncertain effects. Others worry that effects on infrastructure could be longer-lasting and serious.[18]

An essay by Richard Kugler also discusses cyber deterrence.[19] Reviewing the history of U.S. deterrence theory, Kugler notes that the U.S. government even has deterrence doctrine for nuclear forces.[20] My summary of his summary of that doctrine is Table 2.

---

18. *See* Defense Science Board, United States Department of Defense, RESILIENT MILITARY SYSTEMS AND THE ADVANCED CYBER THREAT 2 (2013).

19. Richard Kugler, *Deterrence of Cyber Attacks*, *in* CYBERPOWER AND NATIONAL SECURITY 309 (Franklin D. Kramer et al. eds., 2009).

20. United States Strategic Command, Department of Defense, DETERRENCE OPERATIONS JOINT OPERATING CONCEPT VERSION 2.0 at 17–18 (2006).

TABLE 2. SOME CANONICAL RULES FOR NUCLEAR DETERRENCE: DO THEY APPLY TO CYBER ATTACK?

Specify objectives and context
Assess strategic calculus of adversary
Identify deterrence effects on adversary conduct
Plan and assess courses of action
Develop plans to execute and monitor
Develop capacities to respond flexibly and effectively as matters develop

While the doctrine Kugler points to is admirably sophisticated in many respects, it also has distinct shortcomings. In particular, it is tied to the classic rational-actor paradigm of decisionmaking as suggested by reference to the adversary's "strategic calculus." We know, from decades of research, that much high-level decisionmaking may enjoy "limited rationality" at best and is sometimes driven by heuristics, personality, and emotions.[21] Kugler went on to suggest the elements of cyber deterrence policy as being (1) a clear, firm declaratory policy; (2) high global situational awareness of cyber threats; (3) good command and control; (4) effective cyber defenses, particularly of critical infrastructure; (5) broad counter-cyber offensive capabilities; (6) well-developed interagency and international cooperation and collaboration; and (7) cyber deterrence methodologies, metrics, and experiments to monitor and guide. To be sure, Kugler's essay did not attempt to describe how to do all of these things.

Additional papers have been published over the last few years, of which I will only mention a few. Charles Glaser argues that deterring countervalue cyber attacks may be more feasible than some have suggested, in part because the attribution problem may be adequately resolved by context and character

21. Paul K. Davis, *Toward Theory for Dissuasion (or Deterrence) by Denial*, *supra* note 10. Several papers from a debate in World Politics are still quite relevant. *See, e.g.*, Christopher H. Achen & Duncan Snidal, *Rational Deterrence Theory and Comparative Case Studies*, 41 World Politics 143 (Jan. 1989); Alexander L. George & Richard Smoke, *Deterrence and Foreign Policy*, 41 World Politics 170 (Jan. 1989); Robert Jervis, *Rational Deterrence: Theory and Evidence*, 41 World Politics 183 (Jan. 1989); Richard Ned Lebow & Janice Gross Stein, *Rational Deterrence Theory: I Think, Therefore I Deter*, 41 World Politics 208 (Jan. 1989).

of attack.[22] In contrast, deterring counter-military cyber attacks is problematic because the cyber attacks are likely to be mere components of conventional warfare. Thus, the relevant deterrent challenge is deterring the war overall. One of Glaser's most interesting points is that "[c]ounter-military cyber capabilities would likely increase states' uncertainty about their conventional capabilities, which could make failures of deterrence more likely."[23] Overall, Glaser argues for a combination of persuading the adversary not to attack, defense, and reconstitution and robustness. He says little about cyber offense.

Will Goodman draws on numerous cases to discuss cyber deterrence and its failures.[24] He points out that the well-cited past examples of cyber attack were certainly failures of deterrence, but were less dramatic than sometimes claimed. Although the paper is ostensibly about deterrence (bowing, perhaps, to the common tendency to use "deterrence" to mean everything and nothing), he then covers the influence spectrum of Figure 2 while making clear distinctions. After acknowledging difficulties and failures of deterrence, he speculates about the potential for "defense by futility," i.e., attacks may be dissuaded by a sense that any effects accomplished will prove indecisive (as was argued by Libicki). Goodman also discusses with appropriate ambivalence that economic interdependence and the possibility of attacks being politically counterproductive may or may not prove helpful. He highlights the problem of escalation dominance, arguing that, "[w]ithout escalation dominance, the United States will be left with no recourse in the aftermath of an attack."[25] He does not elaborate, even though the United States does not now have escalation dominance in the cyber realm and is unlikely to achieve it with respect to states like Russia and China. He, like others, argues for a clearer U.S. declaratory policy on

---

22. Charles L. Glaser, *Deterrence of Cyber Attacks and U.S. National Security*, 2011 THE GEORGE WASHINGTON UNIVERSITY CYBER SECURITY POLICY AND RESEARCH INSTITUTE 5, *available at* http://static.squarespace.com/static/53b2efd7e4b0018990a073c4/t/542044fee4b02b592c3ec599/1411400958491/2011-5_cyber_deterrence_and_security_glaser.pdf.

23. *Id.* at 8.

24. *See* Will Goodman, *Cyber Deterrence: Tougher in Theory Than in Practice*, 4 STRATEGIC STUD. Q. 102, 102–29 (2010).

25. *Id.* at 127.

cyberwar, saying that "[h]igher-level strategic attacks and threats should have specific and clearly delineated consequences."[26]

Although agreeing with most of Goodman's paper, I am skeptical about the call for declaratory policy that identifies "clearly delineated consequences" for cyber attack. In the Cold War, the Unites States and Soviet Union deliberately maintained *ambiguity*: NATO prepared carefully for limited nuclear options to re-establish deterrence but, simultaneously, NATO leaders all expressed great skepticism that nuclear war, once begun, could be contained. The result was useful ambiguity. Historically, the so-called "Acheson Dilemma" illustrates the problem that a red line's specificity seemingly identifies everything short of it as allowable.[27] Also, the recent political crisis after Syria used chemical weapons illustrates the political dangers of making red line statements.

A different take on the subject argues for being realistic, leaving deterrence behind, and adopting a full war fighting posture.[28] The authors' conclusion stems from the conclusion that focusing on the cyber deterrence challenge will be fruitless. A key problem is the inherent advantages possessed by the offense in cyberspace, to include advantages related to cover, deception, and mobility. The word "inherent" applies because the internet and related technologies are built on the "opposite default principle" from limiting access. The authors conclude that "[a]cross all measures, cyberspace is an extreme case of an offense-dominated environment. Deterrence is unachievable in such a battlespace."[29] The authors express the hope that, over time, "effective norms against cyberaggression

---

26. *Id.* at 128.

27. In January 1950, Secretary of State Acheson described the U.S. defense perimeter in Asia in such a way as apparently to exclude South Korea. According to lore, Stalin saw a green light and gave the go-ahead to North Korea for its invasion of the South. The lore may be wrong, but the "Acheson Dilemma" is now part of standard education. *See* Donggil Kim & William Stueck, *Did Stalin Lure the United States into the Korean War? New Evidence on the Origins of the Korean War*, THE WILSON CENTER (June 2008), http://www.wilsoncenter.org/sites/default/files/NKIDP_eDossier_1_Origins_of_the_Korean_War.pdf.

28. *See generally* Richard J. Harknett et al., *Leaving Deterrence Behind: War-Fighting and National Cybersecurity*, 7 J. HOMEL. SECUR. & EMERG. MGMT. 1 (2010).

29. *Id.* at 20.

will be important in reining in unacceptable forms of behavior."[30]

The issue of norms is a theme of a more recent paper, which concludes that strategies should concentrate on

> (1) recognizing that crisis instability in cyberspace arises largely from misperception,
>
> (2) promulgating norms that might modulate crisis reactions,
>
> (3) knowing when and how to defuse inadvertent crises stemming from incidents,
>
> (4) supporting actions with narrative rather than signaling,
>
> (5) bolstering defenses to the point at which potential adversaries no longer believe that cyberattacks (penetrating and disrupting or corrupting information systems, as opposed to cyberespionage) can alter the balance of forces, and
>
> (6) calibrating the use of offensive cyberoperations with an assessment of their escalation potential.[31]

To my eyes, Libicki argues (as do I, below) that good sense and accurate perceptions *should* dissuade the worst cyber attacks, but that we cannot count on either of these presently.

The most extensive discussion, albeit with no references to support the many dramatic assertions, is a thoughtful book by Richard Clarke and Robert Knake that reflects Clarke's expert knowledge from lengthy White House experience.[32] The book concludes that

> [w]e cannot deter other nations with our cyber weapons. Nor are we likely to be deterred from doing things that might provoke others into making a major cyber attack. Deterrence is only a potential, something that we might create in the mind of possible cyber attackers if (and it is a huge if) we got serious about deploying effective defenses for some key networks. Since we have not even started to do that, de-

---

30. *Id.* at 22.

31. *See* MARTIN C. LIBICKI, CRISIS AND ESCALATION IN CYBERSPACE, *supra* note 12, at iii.

32. *See* RICHARD A. CLARKE & ROBERT KNAKE, *supra* note 1.

> terrence theory . . . plays no significant role in stopping cyber war today.[33]

Clarke and Knake do not write with a sense of certain doom. They discuss things to do and reasons that cataclysm may well not occur. A major recommendation calls for a defensive triad (improve security of the backbone networks, protect our critical power infrastructure, and improve security of military networks and weapons). They also have ambitious suggestions for international agreement:

> establish a Cyber Risk Reduction Center to exchange information and provide nations with assistance;
> create as international-law concepts the obligation to assist and national cyber accountability, as discussed earlier; impose a ban on first-use cyber attacks against civilian infrastructure, a ban that would be lifted when (a) the two nations were in a shooting war, or (b) the defending nation had been attacked by the other nation with cyber weapons;
> prohibit the preparation of the battlefield in peacetime by the emplacement of trapdoors or logic bombs on civilian infrastructure, including electric power grids, railroads, and so on; and
> prohibit altering data or damaging networks of financial institutions.[34]

The authors are to be congratulated for expressing important ideas, even though some of their specific suggestions will remain controversial. It will be argued, for example, that prohibiting peacetime preparation of the battle space as suggested above would limit U.S. activities but not those of its adversaries, putting the U.S. at a significant disadvantage.

A recent discussion touching on deterrence is a study of improving resilience against the advanced cyber threat.[35] Unlike most of the open literature, this is based on extensive conversation with the information industry and ample access to classified information. A theme in the report is the need to emphasize resilience because fully successful defense is implausible.

---

33. *Id.* at 195.
34. *Id.* at 269.
35. *See* Defense Science Board, *supra* note 18.

In domains where "real" empirical data is lacking, war gaming, red teaming, and related methods have long revealed serious problems that otherwise would have been missed or sloughed off. It is therefore of particular interest to read in the public Defense Science Board (DSB) study that "[Department of Defense] red teams, using cyber attack tools which can be downloaded from the internet, are very successful at defeating our systems."[36] In characterizing the degree of disruption, the report says that "[t]ypically, the disruption is so great, that the exercise must be essentially reset without the cyber intrusion to allow enough operational capability to proceed."[37]

The DSB's description of cyber attack potential is no less alarming than that of Clarke and Knake.[38] As the most tangible measure of the study's concern, the report recommends a deterrent based on a full range of response mechanisms, to include nuclear responses. Their first recommendation is to "Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack)."[39] The term "existential" is important. Only in extreme circumstances might a cyber attack be arguably in the realm of existential. However, the study team saw such an attack as plausible.

The conclusion is controversial. Richard Clarke argues against blurring the distinction between cyber and nuclear threats, believing that such blurring will make cyberpeace even more difficult to attain.[40] Others, like Eldbridge Colby, disagree, arguing that the linkage—even if tentative—would be to encourage stability rather than a notion that cyberwar is a "Wild West" arena where rules are lax or nonexistent.[41]

Kamal T. Jabbour and E. Paul Rattazzi provide another review of cyber deterrence issues, pointing out the same

---

36. *Id.* at 1.

37. *Id.* at 5.

38. *See* RICHARD A. CLARKE & ROBERT KNAKE, *supra* note 1, at 5.

39. *See* Defense Science Board, *supra* note 18, at 7.

40. Richard A. Clarke & Steve Andrasen, *Cyberwar's Threat Does Not Justify a New Policy of Nuclear Deterrence*, THE WASHINGTON POST (July 14, 2013), http://www.washingtonpost.com/opinions/cyberwars-threat-does-not-justify-a-new-policy-of-nuclear-deterrence/2013/06/14/91c01bb6-d50e-11e2-a73e-826d299ff459_story.html.

41. Elbridge Colby, *Cyberwar and the Nuclear Option*, NAT'L INT. (June 24, 2013), http://nationalinterest.org/commentary/cyberwar-the-nuclear-option-8638.

problems mentioned above, concluding that what is needed are new domain-specific approaches to deterrence, including technologically feasible ways to strengthen the infrastructure.[42] Another paper in the same volume draws on deterrence doctrine[43] to describe what the authors see as a necessary "operationally responsive cyberspace," saying that its realization "not only prepares the United States to operate under duress, but sends a strong deterrence message to potential adversaries that the nation aims to deny the benefit derived from an adversary's cyberspace attacks."[44]

B. *Whom To Believe? Is the Sky Falling?*

Even from this brief review it is evident that authors writing on cyberwar differ strongly about the reality and proportions of the cyber threat. A number of scholars, despite being concerned about cyber threats, are very cautious to avoid and deplore hype on the subject, to point out that the effectiveness of many past instances have been overblown, to note the absence of support for some of the more dramatic descriptions, and to discuss the many reasons that should give offensive cyberwarriors pause.[45] High-value cyber attacks by nations require exceptionally detailed information and knowledge to plan, are beset by myriad uncertainties, and are likely to create effects that are only temporary and not decisive. Thus, cyberwar should be seen as part of larger conflict, rather than as stand-alone.[46]

---

42. Kamal T. Jabbour & E. Paul Ratazzi, *Deterrence in Cyberspace*, *in* THINKING ABOUT DETERRENCE: ENDURING QUESTIONS IN A TIME OF RISING POWERS, ROGUE REGIMES, AND TERRORISM 37–47 (Adam Lowther ed., 2013).

43. *See* OFFICE OF PRIMARY RESPONSIBILITY, DETERRENCE OPERATIONS JOINT OPERATING CONCEPT: VERSION 2.0. (2006).

44. Kevin R. Beeker et al., *Operationally Responsive Cyberspace: a Critical Piece in the Strategic Deterrence Equation*, *in* THINKING ABOUT DETERRENCE: ENDURING QUESTIONS IN A TIME OF RISING POWERS, ROGUE REGIMES, AND TERRORISM 35 (Adam Lowther ed., 2013).

45. *See* MARTIN C. LIBICKI, *supra* note 17; Will Goodman, *supra* note 25; Thomas Rid, *supra* note 1.

46. Thomas Rid's criticism also includes deploring reference to "cyberwar" because he interprets "war" to require violence, instrumental purpose, and political nature. Thomas Rid, *supra* note 1, at 8, 11. He also seems to focus on standalone cyberwar. To this author's eyes, his conclusion that "cyberwar will not occur" may be correct with his definitions, but not

As to seriousness, it is noteworthy that those most familiar with the problem from high positions (Secretary of Defense, Chairman of the Joint Chiefs of Staff, Director of the CIA, and "czar" of cyber issues in the White House) are alarmed. In addition to the clarion call of Richard Clarke,[47] former Chairman of the Joint Chiefs of Staff Mike Mullen, not known for a tendency toward hype, testified that "[t]he effects of a well coordinated, state-sponsored cyber attack against our financial, transportation, communications, and energy systems would be catastrophic."[48] The use of "would" rather than "could" was not accidental. CIA Director Leon Panetta, about to become Secretary of Defense Leon Panetta said on June 9, 2011 that

> I'm very concerned that the potential in cyber to be able to cripple our power grid, to be able to cripple our government systems, to be able to cripple our financial system would virtually paralyze this country. And, as far as I'm concerned, that represents the potential for another Pearl Harbor as far as the kind of attack that we could be the target of using cyber.[49]

Since fighter pilots, ship drivers, tank commanders, and elderly political officials have no natural attraction to cyberwar, it is striking that the Department of Defense—even in this period of extremely tight budgets—has been pouring money into cyberwar commands and related force structure. Clearly, the officials' alarm is real; they would bristle about being called alarmist.

The remainder of the Article focuses on how cyber attack and cyberwar are similar and different from past challenges and what the implications may be for deterrence and influence more generally. It ploughs some of the same ground as the authors cited above, but reflects my own take on the subject.

---

when the term "cyberwar" is used more generally as so common in usual discussion.

47. *See* Richard A. Clarke & Steve Andrasen, *supra* note 39.

48. *Posture Statement of Admiral Michael G. Mullen, USN, Chairman of the Joint Chiefs of Staff Before the H. Armed Serv. Comm.*,112th Cong. 17 (2011).

49. Edwin Mora, *Panetta Warns of Cyber Pearl Harbor: 'The Capability to Paralyze This Country is There Now,'* cnsnews.com (June 13, 2012), http://cnsnews.com/news/article/panetta-warns-cyber-pearl-harbor-capability-paralyze-country-there-now.

III. Parallels and Differences

A. *Relevance of Classic Concepts*

Everyone contemplating the strategic consequences of cyber threats tends to draw comparisons with prior strategic thinking, particularly from the nuclear and conventional war concerns during the Cold War. Table 3 shows such a comparison. The left column shows concepts that were important in Cold War discussions of strategy. The subsequent columns show my subjective assessment of their importance in discussing cyberwar issues. Assured destruction and assured retaliation to destroy the adversary's society have low salience because cyberwar is simply not as destructive as nuclear weapons or even large-scale attacks with precision conventional weapons. Further, cyberwar's effects are highly uncertain and would probably be temporary and non-decisive. The crucial Cold War distinction between countervalue and countermilitary targeting, however, is highly salient as discussed by numerous authors.[50]

Strategic stability here refers to the same concept of stability as in Figure 1. In the Cold War, that included avoiding arms races. An interest in normalcy and stability certainly exists today and affects discussion of cyber issues because even "peacetime" cyber attacks by nations, primarily for intelligence, are disruptive and raise tensions.

Table 3. Relevance of Concepts from Cold War Nuclear Strategy

Consideration	*Relevance to Cyberwar*	*Comment*
Assured destruction and assured retaliation	Low	Cyberwar is not in the same league as nuclear war or even kinetic war with precision weapons insofar as "assuring" anything, much less long-term incapacitation or destruction.
Countervalue versus counterforce	**High**	Collateral effects and related confusion are likely.
Strategic stability	Medium	Interest in normalcy, predictability, stability

50. *See generally id.*; *see also* Libicki, *supra* note 17, at 39–42.

Crisis instability	Mixed	Relevance varies with issue: a. Disarming first-strike capability, Low b. Avoiding perceived cost of going second, **High** c. Seeing leverage in surprise attack in limited conventional war (e.g., to deactivate air defenses), **High** d. Considering escalation to re-establish deterrence, **High**
Competitive strategy	**High**	The strategy of driving the adversary to spend vast sums on defense applies strongly to cyberwar. So also, breakthroughs can render prior investments obsolete.
Extended deterrence	**High**	Extending standalone cyber deterrence may be unlikely but cyber capabilities affect extended deterrence via war fighting capability.

Crisis instability is a more complex matter to discuss. There seems to be reasonably broad agreement that cyberwar does not provide a credible disarming first-strike capability. The detailed knowledge required would be stupendous and the uncertainties enormous. It is one thing for a side to contemplate just how awful a full-scale attack *might* be (the existential attack referred to by the DSB study); it is quite another matter to contemplate launching such a problematic attack oneself.

That said, there is emerging consensus of severe crisis instability. Why? It relates to what I call the perceived "cost of going second."[51] Even if a side doesn't believe it has a disarming first-strike capability, it may well be frightened of what would happen if the other side attacks *and* may be convinced that going first will be advantageous, especially with a measure of surprise so that prior "preparation of the battlefield" (e.g., laying logic bombs in enemy networks) could be exploited

51. I discussed this theme and the related concept of "dangerous ideas" (ideas that might actually trigger a nuclear first strike) in a long-ago monograph that appears all too relevant today. Paul K. Davis, *Studying First-Strike Stability with Knowledge-Based Models of Human Decision Making*, RAND (1989).

before the adversary takes measures to change network configurations, processes, and so on. Although the *ultimate* value of going first might be objectively modest because conflict would probably be lengthy and brutal, to committed cyberwarriors and those who have not thought through the matter well, there would be predictable at-the-time pressure to act preemptively and, quite possibly, make overly optimistic assessments of what could be accomplished.

At the height of the Cold War, an analogous preemption would have initiated nuclear war. Senior civilian and military leaders appreciated viscerally the catastrophe that would mean. As a result, they could be expected to override pressures from the ranks to preempt. In the leaders' minds, the cost of going first *unnecessarily* was essentially infinite, outweighing the cost of going second, given that secure retaliatory capability existed. The closest exception is that NATO doctrine emphasized potential escalation to limited nuclear war so as to re-establish deterrence in the event of a Warsaw Pact conventional invasion that was about to succeed.

In the cyber era we should expect that in a sufficiently serious limited conflict (e.g., in the Asia-Pacific region), there would be pressures to escalate. Air-Sea Battle contemplates limited kinetic attack on the Chinese homeland.[52] Some would likely advocate for cyber attack going beyond that which is necessary to support the kinetic operations. The intent would be to re-establish deterrence (i.e., to bring about de-escalation), but the results might well be otherwise. Interestingly, in military war games (albeit with participants with limited experience and responsibilities), it is common to see protagonists reach for "whatever instruments they have available" to avoid losing. They show many fewer compunctions about strategic-level attacks than would have been the case in the Cold War. This is to some extent artifactual, but it is nonetheless sobering. Further, players do not honor boundaries or recognize an equivalent to the Cold War's escalation ladder.

Because the nuclear shadow would be more abstract at the outset of a modern major-power crisis than during the

52. *See* DEPARTMENT OF DEFENSE, AIR-SEA BATTLE: SERVICE COLLABORATION TO ADDRESS ANTI-ACCESS AND AREA DENIAL (2013); *see also* DAVID C. GOMPERT, SEA POWER AND AMERICAN INTERESTS IN THE WESTERN PACIFIC (2013).

Cold War, it can also be expected that the spirit of war fighting will not only be present but potentially dominant, depending on circumstances and personalities. Offense dominates cyberwar and everyone accommodates their thinking accordingly even though the longer-term benefits of offensive cyberwar remain highly uncertain and the longer-term consequences of larger war would almost surely be very bad.

To touch more briefly on additional items in Table 3, some other concepts from the earlier era carry over. The concept of "competitive strategy" that included taking steps forcing the adversary to spend wildly but to no avail on defensive measures has a direct analogue today.[53] Unfortunately, as in much of the latter Cold War period, the United States appears to be at a disadvantage: especially because it has a more integrated network and many fewer state-directed constraints on network use, it will be extraordinarily expensive for the United States to achieve high levels of defense even if it is even possible to do so. Finally, consider extended deterrence. For a half-century or more we have recognized that this is a bigger challenge than direct deterrence because the credibility of the direct-deterrent threat is inherently higher. In the cyber era, the United States might not be able to credibly threaten strategic cyberwar in response to cyber attack on an ally, but whatever capabilities were brought to bear in extending conventional and nuclear deterrence to allies would include cyber attacks.

B. *What Would Be Escalatory? Is There an Escalation Ladder?*

As another point of comparison, consider whether cyber attack would be "escalatory," by analogy to moving up the escalation ladder of nuclear-strategy fame. Table 4 is a simplified way of thinking about this issue. The left column shows level of conflict. The question then addressed in the columns to the

---

53. "Competitive strategy" is a broad concept in the business world but a version has also been influential in defense strategy. *See generally* COMPETITIVE STRATEGIES FOR THE 21ST CENTURY: THEORY, HISTORY, AND PRACTICE (Thomas G. Mahnken ed., 2012). One U.S. success in Cold War competitive strategy was development of stealth capability, which rendered the massive Soviet investment in air defenses obsolete. Another example was that 1980's naval tactics threatened Soviet SSBN bastions, causing consternation and expensive defense measures. Later, the story was less happy for the United States. The costs of maintaining stealth and the cost of ballistic missile defense are very high.

right is whether cyber attacks on the target classes along the top row would be escalatory for a given conflict level. Each cell is divided into a top and bottom part. The upper cell assumes that the cyber attack is "small;" the lower cell assumes that it is "large." Thus, reading the first row of the body, small cyber attacks in peacetime are not escalatory because, regrettably, such attacks are part of the baseline. Even large-scale attacks to collect personal data, intellectual property, etc., are part of the baseline.[54] The same is true for terrorist attacks. Moving downward in the table, if instead we assume that a small-scale conventional war is already underway, then—in this notional treatment—even small cyber attacks might be seen as escalatory if against command and control or homeland infrastructure (even if they had been precedented in peacetime). Similarly, large-scale attacks on tactical systems might be considered escalatory even if lesser attacks had been tolerated.

Moving downward again, the case of large-scale conventional war is instructive. One might think that large "countervalue" attacks on civilian infrastructure would obviously be escalatory. However, if the context were conflict with China and the United States was already striking targets in the Chinese homeland, would Chinese cyber attacks on the U.S. homeland be escalatory? The United States might imagine so, but China would not. Thus, Table 4 suggests that limited cyber attacks, even on the homeland infrastructure and nuclear command and control would not obviously be escalatory to an impartial observer.

Continuing down the table's rows, it might be that a great deal of cyberwar would be regarded, grudgingly, as "to be expected" when occurring at higher levels of conflict—not actually escalatory, just part of the package.

Clearly, these assessments are tentative, subjective, and notional for the sake of a think-piece, but they illustrate complicated issues and note the failure of the earlier escalation-ladder concepts. Cyber attack is not necessarily lower than nuclear attack in terms of some updated "ladder." Indeed, the concept of a ladder no longer works, as comes out in war gaming. Theoretically, something more like a lattice is needed,

54. *See* RICHARD A. CLARKE & ROBERT KNAKE, *supra* note 1.

TABLE 4. CAN CYBER ATTACKS BE ESCALATORY?
A SPECULATIVE ASSESSMENT

New targets / *Current level*	*Size of cyber attack*	*Personal Data*	*Knowledge*	*Tactical Military Systems*	*Command and Control*	*Nuclear Command and Control*	*Homeland Civilian Infrastructure*
Peacetime	Small						
	Large			Escalatory	Escalatory	Escalatory	Escalatory
Terrorist Attack	Small						
	Large			Escalatory	Escalatory	Escalatory	Escalatory
Small-Scale Conv. War	Small					Escalatory	Escalatory
	Large			Escalatory	Escalatory	Escalatory	Escalatory
Large-Scale Conv. War	Small						
	Large					Escalatory	?
Limited Nuclear War (not CV or homeland)	Small					Escalatory	Escalatory
	Large					Escalatory	Escalatory
Limited Nuclear War (CV/ homeland)	Small						
	Large						
General Nuclear War	Small						
	Large						

perhaps one with several dimensions.[55] Ambiguity would remain. I recall vividly from analytic war gaming of the 1980s with artificial-intelligence models attempting to represent su-

55. *See also* NATIONAL RESEARCH COUNCIL, *supra* note 2. I thank Ron Lehman and Stephen Downes-Martin for related discussions in the course of that study. **R**

perpower leaders that "unintended" escalation sometimes occurred because the competing models could reach highly plausible but different interpretations of what the current "level of conflict" was.[56] Something alarmingly similar happened in top-level war games within the United States. At the time, the results were quite sobering to officials, as discussed in an important recent book by Paul Bracken.[57]

IV. A Simple Cognitive Model for Discussing Deterrence

Although a theme of this Article is that we should focus more on broader context and influence than on deterrence narrowly, I next sketch a qualitatively analytic way to discuss cyber deterrence in different contexts.[58] Table 5 describes a simple cognitive model for an adversary with limited rationality. It is the framework for a model of the *adversary's* mental frame. For simplicity, it depicts the adversary as having three options: do nothing different (the baseline), take the action X that we are trying to deter, or do something else. Framing the decision as one of choices among options is part of what makes this a cognitive model of limited rationality rather than a behavioral model. Even if the adversary recognizes that prospects are poor if he takes Action X, taking the action might be attractive relative to alternatives. Conversely, the action might have some attraction, but less than that of some other action. Noting the columns for worst-case and best-case outcomes, we see that this framing is not that of usual "decision theory," where the actor would pick the option with the highest expected subjective utility. Finally, Table 5 allows for alternative

---

56. *See generally* Paul K. Davis, Some Lessons Learned From Building Red Agents in the RAND Strategy Assessment System (RSAS) (RAND Corp., 1989).

57. *See generally* Paul Bracken, The Second Nuclear Age: Strategy, Danger, and the New Power Politics (Times Books, 2012).

58. This discussion draws on earlier work. *See, e.g.*, Paul K. Davis, *supra* note 10. This in turn builds on considerable work over many years that included cognitive modeling of Saddam Hussein and regional aggressors. *See generally* Naval Studies Board and Nat'l Research Council, Post-Cold War Conflict Deterrence (National Academy Press, 1996); Paul K. Davis, *Synthetic Cognitive Modeling of Adversaries for Effects-Based Planning*, 4716 SPIE Proc. Enabling Technology for Simulation Science VI (2002), *reprinted in* Modeling Adversaries and Related Cognitive Biases (RAND Corp. 2002); *see also* Richard A. Clarke & Robert Knake, *supra* note 1.

models of the adversary, here called Model A and Model B. They might differ strongly in their risk-taking propensity because of personality, emotion, or other considerations. Thus, in making their net assessments, they would put more or less mental weight on best-case and worst-case outcomes. Further, they might make different assessments about those outcomes or their likelihoods.

This model departs from normal decision analysis in several respects. First, the net assessment need not be based on expected subjective utility, or even on some kind of linear weighting of the best, most-likely, and worst outcomes. Second, the component assessments may be different from model to model, not because of differences in "preference" or utility, but differences of perception and judgment.

TABLE 5. A SIMPLE COGNITIVE MODEL

	Subjectively estimated with deep uncertainty; qualitative							
Option	Worst-case outcome		Expected outcome		Best-case outcome		Net Assessment	
							Model A	Model B
	Model A	Model B	Model A	Model B	Model A	Model B		
Do nothing different								
Conduct Attack X								
Do something else								

Notes: Net Assessment is a function of the preceding columns and the decisionmaker (e.g., Model A or B)—e.g., on the decisionmaker's risk-taking propensity or passion for the possibility of a best-case outcome.

Cell values might be subjective assessments of outcome on a scale of, e.g., -10 to 10.

This conceptually simple model can be remarkably rich if we take care in estimating the cell values by taking into account, as best we can, considerations of the adversary's information; heuristics, biases, and intuitive thinking; values; differences in perception and judgment; personality; and risk-taking characteristics. Doing so may allow us to do far better than by

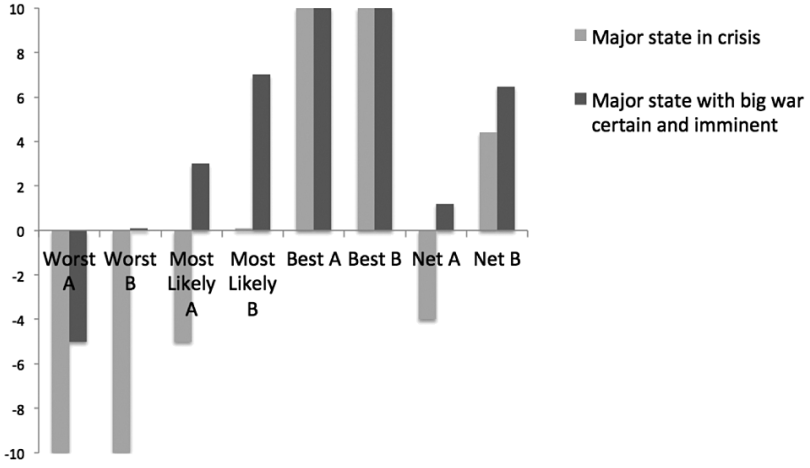
using the classic rational-actor model and its simple-minded "calculus" of comparing options.

Figure 4 is a speculative and qualitative application—simplified to focus merely on the decision to mount a major cyber attack, or not. That is, would mounting such an attack be net positive or negative, compared to not doing so? It does so for two scenarios. In one (light gray), two major nations are in crisis but not yet in war. In the other (dark gray), the states are in crisis but, in addition, big war is regarded as imminent and essentially certain. What will the decision be? Consider two models, A and B, of a government contemplating cyber attack. For the case of crisis without expectation of war, Model A is more cautious about action, seeing a substantial downside (negative outcome) in the most likely case. Perhaps it sees that as making a big war with a very bad outcome likely. That dominates its net assessment, and it decides against initiating cyber attack. Model B's assessments also sees a sizable downside, but believes that the most likely outcome of initiating cyberwar will be "a wash," neither better nor worse than restraint. Further, it sees great *potential* advantage in taking the initiative. That is, its upside assessment (best-case outcome) is very positive. Actually, so is that of Model A, but the difference is that Model B is more risk-taking and puts much more mental weight on the best case. Model B, then, makes a large-scale cyber attack.

Consider next the case in which war is regarded (by both models) as imminent and nearly certain. In this case, both Models A and B would initiate cyberwar, with full expectation of escalation to more general war. Their motivation is simply the belief that whoever goes first with cyber attacks will have a big advantage, which both models believe *might* be decisive (the best-case outcome). Model B sees *no* downside, since going first must be good and war is certain. Model A sees more possibilities, is less sanguine about results, and still sees a bad worst-case outcome, but on balance, decides also to initiate attack. Despite the simplicity and subjectivity of this discussion, it illustrates how crisis instability can be a serious problem for cyber attack. Further, it highlights the way in which perceptions and even psychology enter the problem naturally, rather than being cast in the antiseptic language of the rational-actor paradigm. For example, the differences in how Models A and B assess the best-estimate outcome might correspond to whether proponents of the cyber attack are perceived as

tough, confident, and credible, or as hawkish, over-confident, and non-credible. Such perceptions might be dominated by personalities.

FIGURE 4. PERCEIVED ADVANTAGE OF INITIATING LARGE-SCALE CYBERWAR FOR TWO MODELS



Note: Vertical axis measures outcome value subjectively from extremely negative (-10) to extremely positive (10).

V. CONCLUSIONS

The primary conclusions of this Article are in two categories. Some are intended for scholars and relate to tightening discourse. Some relate to strategy and policy.

Improving Discourse

- "Cyberwar" should be assumed to be war that *includes* cyber attack, rather than war occurring only in cyberspace, unless it appears with a modifier as in "standalone cyberwar."
- The term "deterrence" should be reserved for the classic meaning that involves threat of punishment. What has often been called deterrence by denial should be referred to as dissuasion by denial. Dissuasion by futility should be added to the vocabulary. It is different from but overlaps with dissuasion by denial in that it may operate when an attack cannot be thwarted, but the would-be attacker concludes that, even if temporarily

"successful," the attack would not have the desired consequences because of, e.g., repairs, adaptations, or back-up mechanisms.

- Deterrence should be seen as merely one element along a spectrum of influences, with additional factors at work over which we will likely have no influence. The notion that adversaries can be persuaded not to do something by deterrent threats alone is naive, as is the notion that the driving factors are always within our control.
- Some influences that would affect decisions about cyber attack are outside the usual spectrum of political-military influences. Social and intellectual norms may become part of international "understandings" that mean something even if they provide no guarantees. Given their potential value, it would be unwise to disparage such corresponding options.
- There is need for the analogue to the Cold War's escalation-ladder concept, but that construct will necessarily be multi-dimensional: Cyber attacks may be "higher" or "lower" on the concern scale depending on details of both context and usage.

Strategy and Policy

- Cyber attack and cyberwar are here-and-now national-security threats with the *potential* for catastrophic effect. This is so even though there have been instances of exaggeration in some past accounts of cyber attack; there are limitations of cyberwar that "should" give would-be attackers or escalators pause; and there are reasons for expecting that cyberwar would be disruptive but not catastrophic.
- Deterrent efforts can sometimes play a useful role. Other forms of influence, including laws and social and international norms also have considerable potential for reducing some kinds of cyber attack. Attitudes and norms arguably have more potential than laws per se, but they can be mutually reinforcing.
- Deterrence of cyber attack has failed in the past and will fail in the future. Thus, policy must worry about re-establishing deterrence when it fails and the related concept of cumulative deterrence.

- **Crisis instability is a serious problem because of some actual and substantial perceived first-action advantages. The perceived value of moving first is a *dangerous idea* that should be discouraged by exhortation, cooperation, and measures to reduce the actual value**.

As a final observation mirroring one of the items above, scholars and policymakers should avoid premature conclusions about what actions in the international and legal domains might be useful. Broadly shared concepts, norms, and "rules of the road" can countervail unwise instincts of those subject to the "cult of the offensive." In considering related initiatives, an admonition here is less "trust but verify" than "finding mutual interest can pay off even with those we cannot trust."