AIR UNIVERSITY

AIR WAR COLLEGE

The Ring of Gyges

Anonymity and Technological Advance's Effect on the Deterrence of Nonstate Actors in 2035

DAVID R. IVERSON
Lieutenant Colonel, USAF

Air War College
Maxwell Paper No. 70
Maxwell Air Force Base, Alabama

October 2012

The Maxwell Papers are available electronically at the Air University Press website at http://aupress.au.af.mil.

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

The Ring of Gyges: Anonymity and Technological Advance's Effect on the Deterrence of Nonstate Actors in 2035

Lt Col David R. Iverson, USAF

> "*For all men believe in their hearts that injustice is far more profitable to the individual than justice, and he who argues as I have been supposing, will say that they are right. If you could imagine any one obtaining this power of becoming invisible, and never doing any wrong or touching what was another's, he would be thought by the lookers-on to be a most wretched idiot, although they would praise him to one another's faces, and keep up appearances with one another from a fear that they too might suffer injustice."*
>
> —Plato's *Republic*

From the time of Plato, men have pondered how an individual would act if they were unidentifiable or anonymous. In *The Republic,* Plato used the story of Gyges of Lydia, who found a ring in a cave and put it upon his finger to become invisible to show how a man would act when he believed himself to be anonymous. Gyges used the ring to take over a kingdom becoming the first in a long history of men who altered their actions when they believed themselves to be unidentifiable.[1]

Twenty-four–hundred years later the problems of anonymity that Plato imagined through fiction are becoming reality relative to how they affect deterrence strategies. As technology proliferates and more people and things become connected through networks, individuals are gaining the ability to anonymously become highly disruptive, thereby creating a degree of sanctuary no matter where they reside. As the United States

considers its future deterrence strategy for the 2035 timeframe, understanding how the rapid increase in technological know-how combined with anonymity will affect the behavior of groups and individuals is of paramount importance. Without an improved understanding of this dynamic among groups and individuals, traditional approaches to deterrence may become ineffective by 2035 as anonymity and technological advances constrain a state's ability to use punishment and increases the challenge of denial as currently understood and practiced.

Accordingly, this paper explores the effects of anonymity and technological advances on deterrence theory and recommends ways to make today's deterrence methods more effective in this future environment. It begins by examining the main themes of classic deterrence in the national security literature as they apply to groups and individuals. Next, it presents a basic model of group and individual behavior to explain how anonymity creates an ungoverned space that traditional deterrence strategies do not address. Finally, it recommends two approaches to deter groups and individuals in an anonymous world by (1) increasing the degree of transparency in the actions of individuals globally to reduce their motivation, capability and opportunity to launch attacks; and (2) taking steps to immunize or improve the resiliency of the United States and its allies to deny would-be actors the benefit of their action.

To understand why improved global transparency and immunization will become a pressing national security requirement by 2035, it is first necessary to examine the limitations of current deterrence theory when dealing with issues of groups/individuals and anonymity.

Why Traditional Deterrence Breaks Down in an Anonymous World

For those not wholly familiar with the strategic deterrence literature, deterrence is a strategy designed to prevent an adversary from taking a particular action or series of actions. Deterrence, in its classic state-on-state view, is achieved through two distinct strategies, punishment and denial.[2] Punishment strategies threaten attacks against a nation's population and/or industry to dissuade the actions of an attacker through increased costs. Denial strategies attempt to thwart action by negating the benefits an adversary seeks to gain.[3] The fundamental assumption underpinning both of these strategies is that the threat is definable and identifiable. Remove this assumption and both strategies run into problems.

Punishment

Deterrence by punishment is actively holding an adversary accountable for its actions by threatening to destroy something it values in order to deter its actions.[4] This discourages the adversary from attacking by raising the cost of the attack beyond what it is willing to pay.[5] To accomplish this, deterring nations must be able to (1) identify

the adversary; (2) find something the adversary values; and (3) hold it at risk in a credible way. Historically, states knew who their adversaries were. From ancient times to the Cold War, populations and/or industries were easy targets.[6]

A punishment strategy is difficult to employ against groups and individuals. First, attribution is much more difficult as perpetrators are difficult to identify. The proliferation of technology complicates this task even more, since technological advances allow individuals to gain capability and act anonymously without prior detection.[7] This sanctuary precludes a state from identifying specific would-be attackers, complicating communication of a retaliatory threat. Even if states identify specific actors, they must still find something of value and hold it at risk. For many nonstate aggressors, this is a small target set. In rare circumstances, it may be the nation state's population where they live. In most cases, it is their family or friends, who may be as difficult to find as the actors.

Executing an effective punishment strategy against individuals and groups, therefore, poses challenges and ethical dilemmas for states, particularly when actors are nebulously defined or anonymous. The burden of proof required to identify individuals, or show that a nation-state or civilians are complicit in terrorist activity, is extremely high. Punishing the wrong target is potentially counterproductive, since it may build support for terrorist organizations rather than diminish it. From a

moral or legal standpoint, states may not want to target civilians simply because a potential terrorist values them. These limitations make deterrence by denial a more attractive alternative.

Denial

As opposed to deterrence by punishment, deterrence by denial is designed to make it difficult for an adversary to "attain its political objectives or territorial goals."[8] It can be implemented by actions that minimize or negate the desired effects of an attack, so that the adversary is unable to achieve the objective through violence.[9] This is typically accomplished through defensive measures to improve the resiliency of the civilian population or disarming an opponent (i.e., Cold War civil defense and missile defense). The theory of deterrence by denial assumes the potential opponent and his or her capabilities are known. This awareness—this transparency—allows denial efforts to be tailored against those capabilities posing a danger.

Although deterrence by denial has fewer challenges than deterrence by punishment in the context of groups and individuals, anonymity decreases its effectiveness. For example, one denial strategy might prevent an actor from obtaining attack capabilities while another denies an attack opportunity. However, advancing technology and knowledge, particularly in the fields of biology and genetics, are proliferating rapidly, and along with it, the power of individuals to develop state-like capabilities.[10] The knowledge and materials to create

these capabilities can be obtained anonymously, making denial efforts, such as export or technology controls, problematic.

The size and scale of a denial strategy also make it problematic to prevent an attack opportunity, particularly against anonymous actors. A military truism from Frederick the Great recognized "he who attempts to defend too much defends nothing."[11] Yet group or individual actors, armed with high technology and knowledge, have a huge number of targets to choose from making it difficult to identify an attack location. This large target set makes it difficult to protect everyone from an exhaustive list of potential actors and attack methods.

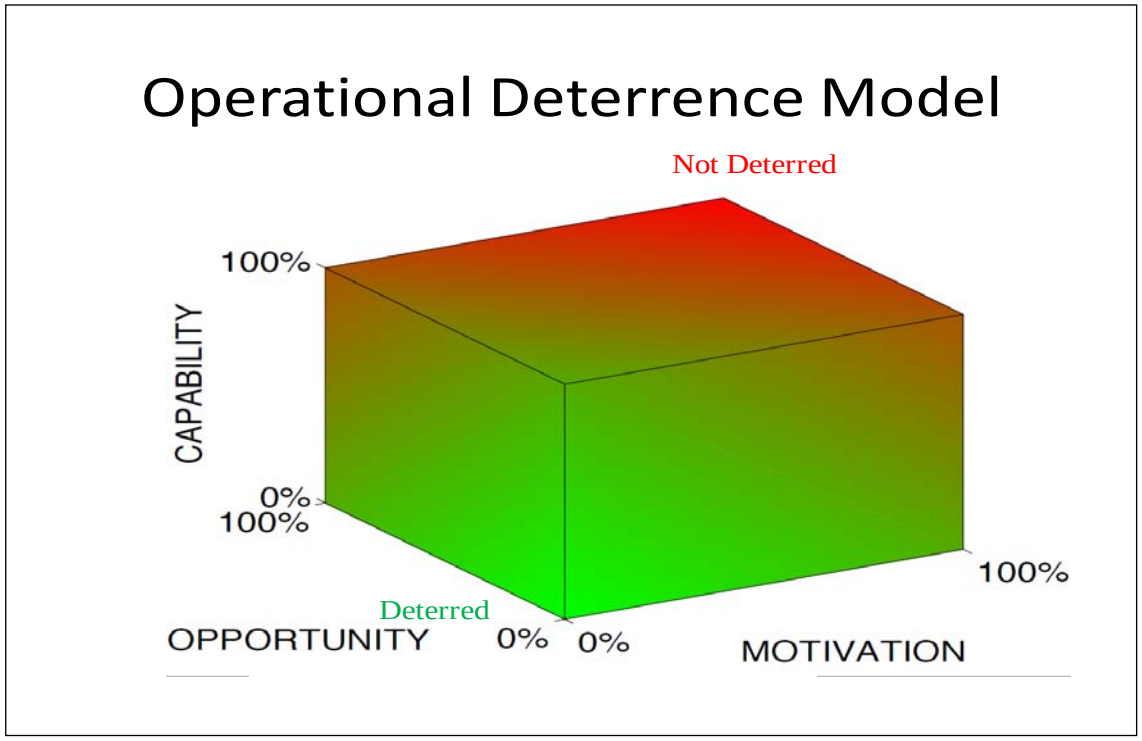
In summary, the traditional state-on-state approaches of deterrence by punishment and denial run into problems in the anonymous world of 2035. Deterrence by punishment seems a nonstarter, particularly for western democracies. On the other hand, deterrence by denial retains some relevance and offers options, but is not sufficient in its current form to deter anonymous groups and individuals. Successful deterrence against groups and individuals in 2035 requires new models and new tools to augment denial. To explore what these solutions might be one must first gain a more indepth understanding of why groups and individuals attack and how anonymity and technical change impact their reasoning.

Why Groups and Individuals Attack

To carry out planned/premeditated or intended attacks, aggressors go through either a four or six step process. John Horgan breaks the lifespan of an attack into a four step process: (1) decision and search activity-targeting and "preterrorism;" (2) preparation or "preterrorist" activity; (3) event execution; and (4) post-event activity and analysis.[12] Taking this model one step further, the Federal Bureau of Investigation uses Calhoun's six-step model to assess attacks which consists of grievance, ideation, research planning, preparation, breach, and attack.[13]

Combining these models produces a three-axis operational deterrence model displaying the interaction of capability, motivation, and opportunity toward deterring violence. This paper uses the operational deterrence model framework (fig. 1) to analyze why groups and individuals attack.[14] The model consists of three axes: X—motivation (grievance, ideation); Z—capability (research/planning, preparation), and Y—opportunity (research, breach, attack). Deterrence fails when an actor is motivated to attack, has the capability, and gains the opportunity. When any or all of the levels of capability, motivation, and/or opportunity are decreased, the likely success of deterrence improves. By examining each axis and applying the model against groups or individuals, specific actions to increase the effectiveness of deterrence can be achieved. The design of new stratagems for deterrence of groups

and individuals in 2035 begins with gaining a deeper understanding of these steps, starting with how motivation affects an actor's decisions and



the role of anonymity in shaping this motivation.

Figure 1. Operational Deterrence Model. (*Adapted from* Grant Hammond, Center for Science and Technology, Maxwell AFB, AL, interview by the author, 11 January 2011.)

Motivation and the Role of Anonymity.

Understanding an attacker's motivation not only explains the veracity of attacks one seeks to deter, but might also signal the risk an attacker is willing to take. One of the preeminent scholars on terrorism, Brian Jenkins, wrote in the 1970's, "terrorists want a lot of people watching but not a lot of people dead."[15] Jenkins's reasoning was that terrorists, such as the Irish Republican Army, sought modest political reform. Therefore, their attacks had to be dramatic enough to undermine

the government and rally people to their cause, but not so dramatic as to undermine their popular support and turn people against them.[16]

The 1990s marked a shift in terrorist thinking for some groups, based on changes in their underlying motivation.[17] While some terrorists still adhered to the "lots watching/few dead" strategy, others sought bolder, more dramatic shifts than incremental political change.[18] Worse, the risk of backlash from large-scale civilian deaths did not deter these groups.[19] This more aggressive strategy opened the door to 9/11 and exploration of weapons of mass destruction (WMD) uses by terrorist groups.[20] While this logic is consistent with commentaries on the political nature of war, what may be less well known is how anonymity affects the motivation of these actors.

Conventional wisdom and initial psychological studies seem to support the assumption that anonymous individuals act more aggressively and are therefore more likely to carry out attacks.[21] Anyone reading aggressive posts on Internet blogs recognizes the potential validity of this argument.[22] However, this conventional wisdom is overly simplistic and slightly flawed when considering anonymity's impact on motivation.

Modern research highlights de-individuation as a more accurate enabler of individual motivation. Deindividuation, of which anonymity is a part, is a psychological state "characterized by diminished self awareness and self-evaluation and a lessened concern for the evaluation

of others."[23] It shows that individuals who believe themselves to be anonymous may not be susceptible to the normal psychological effects of deterrence under the right conditions.

Under normal conditions, deterrence works when individuals (1) share common knowledge of the rules and social logic of the game; (2) engage in tacit and explicit communication (the exchange of information not efforts at collective understanding); (3) accurately assess risks, costs, and gains of strategic games; and (4) control their emotions.[24] Deindividuation interrupts this rule set as individuals no longer apply the same social logic and risk assessment. Although many experts disagree over the causes of deindividuation and the level of antisocial events, a deindividuated state caused by some combination of anonymity, group presence, altered responsibility, and autonomic arousal appears to increase violence and aggressive acts by individuals.[25] This is seen in individual psychological case studies, studies of various non-Western cultural groups, and by looking at modern day terrorists.[26]

Overall, deindividuation reduces self-consciousness and self-inhibition causing individuals to rely on external sources, such as their affiliated group, for direction. Downing and Johnson's 1979 study using individuals associating themselves with groups (through anonymous costumes) as either the Ku Klux Klan (KKK) or nurses showed a definitive group identification effect on aggression.[27] Individuals identifying themselves with the KKK were more aggressive and violent than those in

the nursing group. The individuals took on the group characteristics with which they identified, and aggressiveness either increased or decreased depending upon the group identity.[28] In addition, a 1998 meta-analysis of 60 psychological studies show that individuals tend to act more aggressively and violently when they achieve a deindividuated state. Further, the analysis found when accountability was reduced through anonymity, greater antinormative behavior was induced by following group norms. The end result shows group circumstances appear to be a driving factor for an individual's actions once they achieve a deindividuated condition, either positively or negatively.[29]

Deindividuation's effects also appear to be cross-cultural. A 1973 study based on data from 27 cultures suggested a significant pairing between deindividuation (through some type of change to their physical appearance) and aggression in warfare. For example, cultures altering their appearance through war paint showed an increase in aggression and ferocity over those that did not.[30]

Modern terrorist examples, such as the IRA, show greater proclivities toward violence when they achieve a deindividuated state. [31] In the case of the IRA, terrorism expert A. P. Silke demonstrated that when IRA terrorists used some type of disguise, the crimes they committed showed increased levels and varieties of aggression. This was especially seen in the increased severity of the injuries inflicted upon

victims compared to the crimes committed by IRA members not wearing disguises.[32]

In summary, there is convincing evidence that motivation is directly affected by the psychology of anonymity and deindividuation which, in turn, affects the prospects for deterrence. From a psychological perspective, individuals achieving a deindividuated state through a lack of perceived personal accountability may be more likely to act violently depending upon their group identification.[33] Their motivation is encouraged and enabled by anonymity making them act on their grievances in a violent manner. Therefore, discrediting certain groups' beliefs and establishing a sense of accountability for these groups comprises one component of an updated deterrence approach for groups and individuals. More clues lie in the second area of the paper's analytical framework, anonymity's effect on capabilities.

Capability and the Sanctuary of Anonymity

The second area states must consider when deterring groups and individuals is how anonymity and technology impact the research, planning, and preparation components of an attack. S. Paul Kapur's essay "Deterring Nuclear Terrorists," explores deterrence against nonstate actors in a nuclear weapons context.[34] Kapur's argument compares the relative wealth of actors with their goals in analyzing the effectiveness of a punishment and denial strategy (table 1).[35]

Table 1. Summary table of S. Paul Kapur's thesis

Current Actor Situation	Rich	Poor
Positive Goals (seeks to advance the welfare of an existing population or territory	Denial is hard Punishment is possible	Denial is easy Punishment is possible
Negative Goals (seeks maximal violence and destruction)	Denial is hard Punishment is unlikely	Denial is easy Punishment is unlikely

As long as cost remains a barrier to technological access, Kapur is correct in differentiating rich and poor actors regarding the ability of a deterrence strategy to work against them. However, by 2035 technological development will lower technological cost and blur the lines between rich and poor, calling Kapur's main arguments into question. As the level of technology increases, the cost of acquiring technologies like biological weapons capability may no longer be prohibitive. Technological advances will enable individuals or groups to access information, research, and materials more cheaply and easily than ever before while helping to maintain their anonymity. Moreover, falling costs reduce financing requirements allowing many groups to participate, making a catastrophic attack more difficult to deter.[36]

This scenario is made worse by the impact of anonymity. As previously discussed, deindividuation interrupts the rule set underlying deterrence. Instead of a rich versus poor discriminator, technology may make an individual's anonymity a determining factor in his calculus to

carry out an attack, calling into question the effectiveness of deterrence strategies (table 2).

Table 2. Technological advances and anonymity's effects on classical deterrence

Future Actor Situation	Anonymous	Identifiable
Positive Goals (seeks to advance the welfare of an existing population or territory)	Denial is unlikely Punishment is unlikely	Denial is hard Punishment is unlikely
Negative Goals (seeks maximal violence and destruction)	Denial is unlikely Punishment is unlikely	Denial is hard Punishment is unlikely

Although groups and individuals may be capable of a wide range of WMD attack options to include nuclear, biological, cyber, and chemical, biological weapons hold the most potential danger for the United States in the 2035 timeframe.[37] Unlike nuclear weapons, which require industrial facilities to produce the fuel, the production of biological weapons will be easier for individuals or small groups. In the past, nuclear or biological weapons programs required the resources of a state and the knowledge of highly educated individuals.[38] Countries such as the former Soviet Union have invested enormous amounts of resources in the research and development of biological weapons.[39] With technological advances making research and knowledge from the fields of genetics and synthetic biology more easily accessible (and able to be acquired anonymously), individuals and small groups could gain the ability to carry out attacks that can cause mass casualties.[40]

The implications of these developments are grave in today's terms. Sanctuary or safe havens are thought of in geographic terms—ungoverned space provided by a rogue or failing state.[41] In the future, technological developments in the biological sciences may provide sanctuary in plain view, with would-be attackers anonymously developing genetically altered pathogens using inexpensive common items and knowledge from the Internet. Those anonymously accessing publically available information or purchasing common materials become harder to identify and may operate with impunity no matter their location, becoming harder to deter. As with motivation, combating this threat requires an updated deterrence approach combining elements of denial with tools to create the perception of accountability. If governments fail to do this, the final chance for deterrence centers on denying opportunity.

Opportunity and the Advantage of Anonymity

Once individuals or groups acquire the motivation and capability to carry out a catastrophic attack, they move into the breach and attack phase. They begin looking for the opportunity to conduct their attack with the capability they have acquired. During this phase, they attempt to find the best way to carry out an attack, breaching any known security.

In many ways, deterring at the opportunity phase is too late. Ubiquitous technology and knowledge makes everyone a potential

attacker, requiring elaborate and costly measures to deny an attack opportunity. At the same time, anonymity makes it exceedingly difficult for governments to discern likely attackers and their potential targets without a focused effort. Moreover, capabilities such as biological weapons allow the aggressor to attack on the perimeter, unseen, without penetrating defensive measures. An attacker only needs to infect unsuspecting civilians with an undetectable virus that spreads through normal societal interaction, effectively bypassing any security measures set in place.[42] Because of insights like this, the next section of the paper explores the new tools and techniques states will require to deter anonymous actors in 2035.

Deterring Groups and Individuals: Expanded Denial Strategies

In order to continue using deterrence as an effective strategy against groups and individuals, the United States needs to address the challenges of motivation, capability, and opportunity created by technical advancements and anonymity (fig. 2). In the near future, given the nature of emerging threats, deterrence strategies targeting the motivation and capability of actors may have the greatest chance for success. At the same time, strategies focused on denying opportunity may become increasingly difficult, especially given amorphous threats such as those posed by biological weapons.

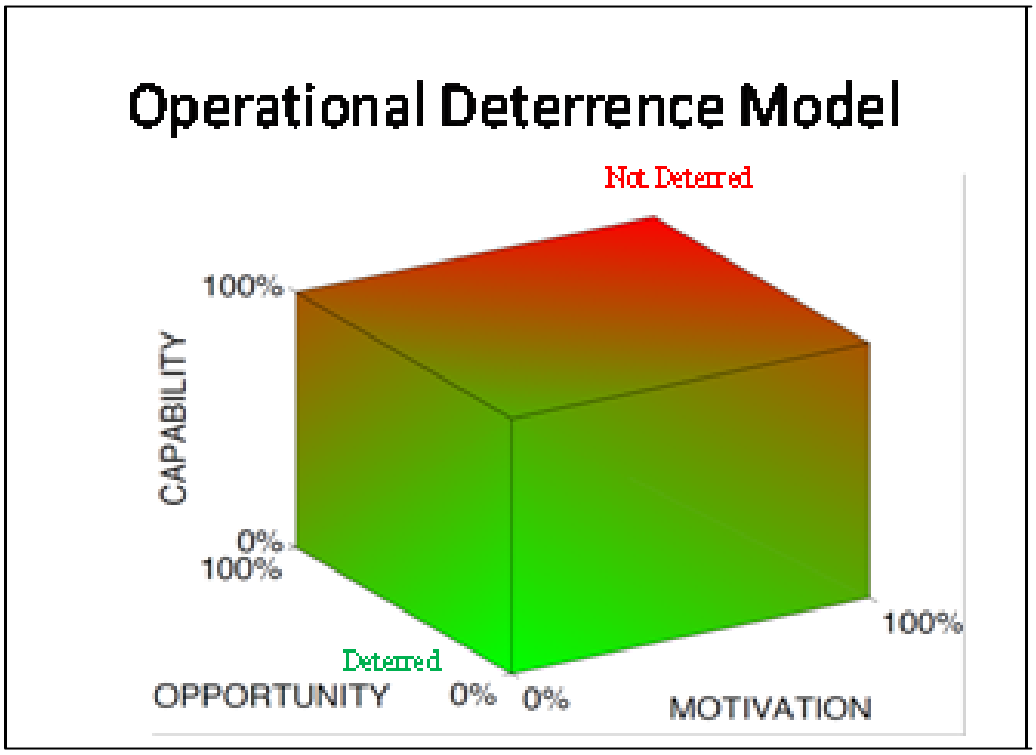


Figure 2. Operational Deterrence Model

Although technological advances threaten traditional deterrence strategies, they may also enable a strategy of expanded denial that better addresses the threat posed by groups and individuals. Two tools enable such a strategy. The first tool, transparency, provides the ability for the government to see, scan, and share virtually all available information from public and private data. The goal of transparency is to negate the effects of anonymity on deterrence. By creating the perception within a watched targeted group, a state may be able to diminish the motivation of its members and minimize deindividuation, making it more difficult for the group to develop harmful capabilities and increase the odds of detection during execution.[43]

The second tool, called immunization, envisions creating a resilient nation, both physically within its infrastructure and cognitively within its population. The goal of immunization mitigates the effects of an attack quickly in order to maintain the trust of the population in its government. If the government can create the perception that it is immunized, successful attacks—one that strikes wide-spread panic or overcomes the capability of government to respond—may become so difficult that they diminish motivation or increase detection odds as groups attempt to develop more elaborate attacks.[44] A more indepth discussion of each of these tools highlights their synergistic interaction with one another.

How Transparency Expands Denial Options

Transparency enhances denial by reducing an actor's motivation, capability, and opportunity. Transparency affects motivation by reducing anonymity and deindividuation. As this paper has shown, anonymity tends to promote deindividuation which, in turn, tends to increase motivation. Removing anonymity reverses the cycle: deindividuated individuals become individuated; motivation is reduced, and the "normal" deterrence calculus is restored.

Similarly, transparency affects capability and opportunity by creating the perception (or reality) of surveillance. This may deter suppliers from providing critical components or individuals from accessing certain information in the public domain. Moreover, it may

affect opportunity as well, convincing individuals to delay or alter their plans prior to execution.

Transparency is operationalized through several lines of operations graphically (fig. 3). The first is through the development of a global information exchange system that uses all-source public and private data to identify and track tens of thousands of individuals who may be likely to carry out attacks. The most effective way to prevent an act of terrorism may be to reduce the individual's motivation to carry out the attack in the first place. Developing a system that catalogs and tracks the electronic interactions of targeted individuals and makes its existence known may create enough doubt in the mind of the would-be attacker to deter/reduce motivation. Moreover, this degree of transparency aids in targeting strategic communications efforts, preventing the first step toward intended violence.[45] At a tactical level, individuals reindividuated through transparency may be persuaded by the social norms of society that their actions or the actions of their affiliated groups are not acceptable, changing their ideation of violence as an acceptable method for attaining their objectives.[46]

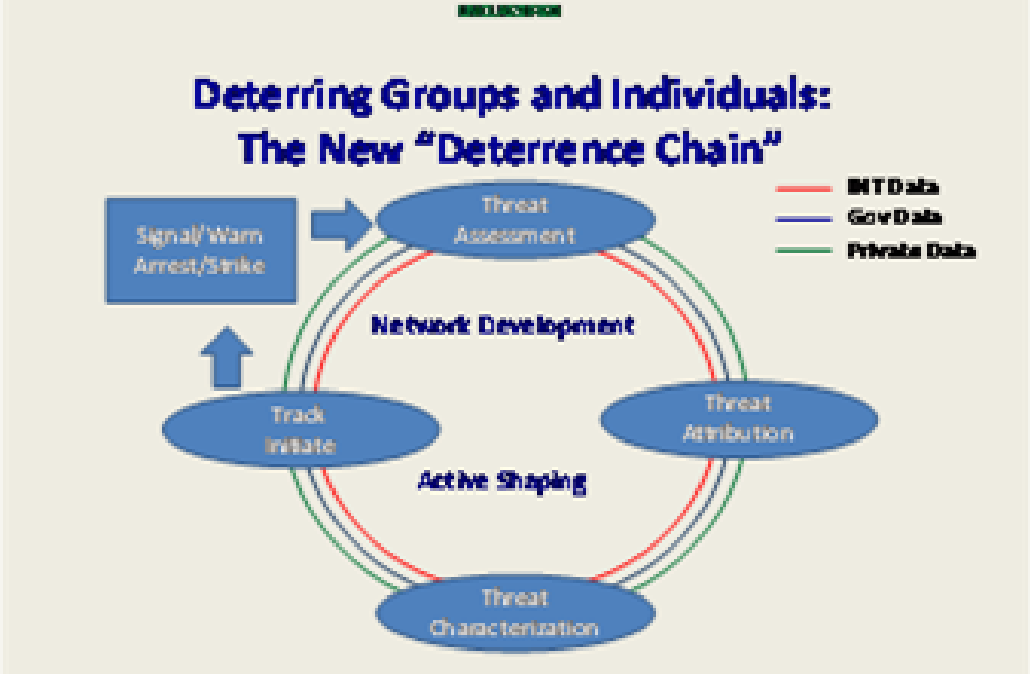


Figure 3. Deterrence Chain.

The second line of operation is a focused effort aimed at denying harmful actors the required capability to carry out an attack. Specifically, the government must prevent the acquisition of critical information or components by removing the sanctuary of anonymity through a two-tiered approach. The first tier leverages tracking the activities of potentially hostile groups and individuals. By monitoring the electronic activities of these individuals, illicit behavior can be quickly identified and acted upon.[47] The second tier involves tracking information and things: who accesses critical information, who manufactures items of interest, and who purchases items of interest. For example, individuals accessing critical information for the construction of nuclear or biological weapons need to be identified and vetted. Likewise, critical components or materials that create "chokepoints" for the

manufacture of these weapons need to be identified and tracked when they are acquired. The results of these efforts connect the dots when actors of concern come into contact with information and materials of concern.

The third line of operation is focused on curtailing opportunity, when it is possible. In this line, traditional "at the wire" physical security measures are enhanced through active shaping efforts aimed at creating a sense of surveillance. If a group can be led to believe that their identity is known, then their perceived risk level in carrying out an attack is heightened and may deter. These enhanced efforts to deny opportunity also work in conjunction with previous efforts to influence and alter the motivation of an actor.[48]

The fourth and final line of operation is focused on physical enforcement. The United States must be ready to deny an attack by arresting or killing hostile actors. Transparency will make this happen more easily. Not only may this stop a specific act but denying specific opportunities in this manner will have an effect on the motivation of other actors bringing deterrence full circle.[49] The best example of targeting individuals is evidenced in Israeli Defense Force operations.[50] These operations have been arguably successful and Israeli governments as well as academics, such as Stephen David and Daniel Byman, argue that terrorist targeting deters future attacks.[51] While transparency uses

technology and actions to reduce the perception of anonymity, immunization aims to make it less relevant.

How Immunization Expands Denial Options

In addition to transparency, immunization is another tool enhancing denial. It is most effective when focused against an actor's motivation and opportunity. Mitigating the effects of attacks by immunizing the population and high value infrastructure may deter individuals and groups from acting by denying them the desired results of their attack. This will reduce their ideation of violence as an effective way to attain their goal. Specifically, the United States should build a more resilient, immunized society by creating the ability to prevent or mitigate catastrophic attacks as well as desensitize its citizens to smaller scale terrorist attacks.

By building a national immunization system to deal with a catastrophic terrorists attack, the government practices deterrence through denial by taking away the terrorists' motivation to paralyze the population through a sensational event and prepares Americans to deal with a smaller attack. To do so, the government must change the public perception about attacks by nonstate actors and prevent overreactions.[52] The current emphasis of the United States on the prevention of all terrorist attacks regardless of scale is an admirable goal, but perhaps not the correct approach. In the future, it may not be possible for both fiscal and operational reasons. In order to accomplish the thwarting of all

terrorist attacks, the government will have to be right 100 percent of the time, an impossible task. Therefore, the American public needs to be educated to accept the possibility of small scale terrorist attacks, while at the same time preparing to survive a catastrophic attack if it occurs. This denial effort will affect the motivation of nonstate actors by denying them their motivation and potentially preventing future grievances of perceived actions against them, their families, or affiliated groups.[53]

The United States must further immunize against an actor's motivation by significantly increasing its capability to detect, identify, and counteract attacks such as a biological threat. Advanced detection systems need to be designed to monitor air and water contaminants across America. Medical facilities should be networked to recognize the signs of a biological outbreak. This must be done with the implementation of sensors everywhere, such as in cell phones or motor vehicles,[54] and the sharing of information through a transparent network. Here the synergy of transparency and immunization work together. Once identified, the American government should be able to decode, prototype, manufacture, and distribute a vaccine within 72–96 hours of detection.[55]

Research should focus on how to detect, decode, and prototype a biological agent vaccine, while coordination with pharmaceutical companies will enable efficient vaccine mass production once it is prototyped. At the same time, designing a logistics system that is

organized and rehearsed to distribute a vaccine will save vital hours. With this capability in place and publicized through transparent strategic communications, terrorists' motivation will be deterred because their attacks may not succeed and may only kill those that the United States decided not to inoculate with a cure, a possibility that should be communicated as part of transparent strategic communications.

While lessening individuals' motivations, an expanded denial strategy should also lessen actors' opportunities to carry out an attack, bringing its success into question. Opportunity will be thwarted through direct security measures enacted to stop an attack, such as preventing weapons from being brought into an area or blocking viruses from infecting a network. Due to the expense, this form of denial may require it to be used to protect only the most critical targets and may require supplemental government financing of commercial companies. In addition, publishing real or imaginary defenses, at times specifically and others vaguely, may cause an increase in an individual's uncertainty, bringing into question their ability to breach those defenses.[56] During the opportunity phase, the synergistic combination of a transparency system with immunization effects of security measures creates a greater chance for deterrence.

More research and studies are needed to answer questions for policy makers as they contemplate deterrence through expanded denial against individuals and groups. Scholars must consider the legal

limitations, such as the Fourth Amendment, and what limitations the ideas of transparency have within the US Constitution. In addition, studies must be accomplished to better understand what response times are required to prevent a biological disease from killing millions. Greater research is also required to determine the effectiveness of terrorist targeting in the long run.

Finally, policy makers need to recognize that denial is the dominant strategy against individuals and groups. In order to be successful an enhanced denial strategy using the tools of transparency and immunization must focus on motivation and capability. This will require a "whole nation" approach, implemented simultaneously by all parts of the government and selected corporations. As one example, the Department of Defense must use its expertise in systems integration, command and control, mobility/logistics, and crisis response to collect and integrate information creating greater transparency and prepare attack responses, creating greater national immunization.

Conclusion

Technological advances over the next 25 years and the anonymity they will allow have the capacity to make deterrence theory ineffective in the 2035 timeframe. Individual or small group nonstate actors may have the technological capability and the psychological frame of mind to carry out catastrophic attacks. To successfully deter these attacks, the United States must work against hostile actors' motivation, capability, and

opportunity by using transparency and immunization. Transparency must identify an actor or make an adversary believe that he or she has been identified; altering his or her motivation, preventing the capability to carry out an attack, and calling into question the opportunity for a successful attack. At the same time, an immunization strategy must deter motivation by reducing grievances and the ideation of violence as the answer. An immunization strategy during the opportunity phase, working in conjunction with transparency, may reduce the likelihood of a successful attack and may lessen the motivation of an actor. If states incorporate these ideas, deterrence theory will still hold a prominent place among the strategies the United States uses against individuals and groups.

Notes

1. Plato, *Republic*, 2nd ed. and trans. G. M. A. Grube and C. D. C. Reeve (Indianapolis, IN: Hackett Pub Co, 1992), 34–38.

2. John J. Mearsheimer, *Conventional Deterrence* (Ithaca, NY: Cornell University Press, 1983), 14–16.

3. Ibid., 14–15.

4. Glen H. Snyder, *Deterrence and Defense, Toward a Theory of National Defense* (Princeton, NJ: Princeton University Press, 1961), 14–16.

5. Ibid.

6. Thucydides, *History of the Peloponnesian War*, trans. Rex Warner (London, UK: Penguin Books Ltd, 1972), 400–407; and Frank Miller, "Disarmament and Deterrence: A Practitioner's View," in *Abolishing Nuclear Weapons: A Debate*, ed. George Perkovich and James M. Acton (Washington, DC: Carnegie Endowment for International Peace, 2009), 149–55, http://www.carnegieendowment.org/files/abolishing_nuclear_weapons_debate.pdf. The *History of the Peloponnesian War* contains the first recorded historical example of an adversary holding a population at risk to achieve its objectives. The Melian dialogue between the Athenians and the Melians of Melos offered the Melians the choice to either surrender and join their alliance or be destroyed. The Melians were just a pawn in the Athenian strategy of deterring other allies from rebellion or joining with the Spartans by using them as an example. During the Cold War nuclear weapons were used at the core of a deterrent strategy by the United States. They proved useful in creating a stable world order which deterred the great powers of the United States and the Soviet Union from unrestrained conflict.

7. William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, 15 January 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.ht

ml. Individuals and groups acting anonymously can best be seen in the cyber world. The Stunex attack against the Iranian nuclear program and multiple denial of service attacks against international corporations are examples of what individuals and groups can do anonymously.

8. Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 12–17.

9. Mearsheimer, *Conventional Deterrence*, 14–15; and Glenn Snyder, *Deterrence and Defense*, 14–16.

10. Barry S. Pallotta and Michael S. Finnin, "DIT Biology: Capability Assessment" (briefing, Institute for Defense Analysis, Alexandria, VA, 4 May 2010), 2–26.

11. Frederick the Great, *Frederick the Great on the Art of War,* ed. and trans. Jay Luuvas (New York, NY: Da Capo Press Inc., 1966), 120.

12. John Horgan, *Psychology of Terrorism* (New York, NY: Routledge, 2005), 109–20.

13. Frederick Calhoun and Stephen Weston, "Managing Threats; Reducing the Risk of Violence" (seminar, Specialized Training Services, San Diego, CA, 2009), 6–11.

14. Grant Hammond (Center for Science and Technology, Maxwell AFB, AL), adapted from interview by the author, 11 January 2011.

15. Brian M. Jenkins (RAND Corp, Santa Monica, CA), interview by the author, 29 November 2010.

16. Ibid.

17. Brian Michael Jenkins and Paul K. Davis, *Deterrence and Influence in Counterterrorism* (Santa Monica, CA: RAND, 2002), 4, 39–43.

18. Horgan, *The Psychology of Terrorism*, 23–46; and Jenkins, interview. Psychological research into nonstate groups/individuals using terrorism has created no definitive profile for who is most likely to carry out violent acts in order to achieve their political objectives but has given clues as to what motivates them. Some fascist groups such as al-Qaeda desire to carry out catastrophic attacks against the United States and its allies. Such fascist groups have a grievance against the United States and have arrived at the idea that violence is the only way to achieve their goals. The United States is seen as the cause of injustice and the root of all that is wrong with their countries, their ethnic group, or their personal situation. In turn, some individuals and groups believe that if they can impose severe damage against the United States, thereby raising the costs to an unbearable level, they will be able to achieve their political goal of creating a new ruling order.

19. Jenkins, interview.

20. "Al-Qaeda Cell Killed by Black Death was Developing Biological Weapons," *Telegraph.co.uk*, 20 January 2009, http://www.telegraph.co.uk/news/worldnews/africaandindianocean/algeria/4287469/Black-Death-kills-al-Qaeda-operatives-in-Algeria.html. In

January 2009, 40 terrorists were found dead in a training camp in Algeria. The al-Qaeda group is suspected to have been killed by a plague as they were attempting to develop biological weapons.

21. Jamie Madigan, "The Psychology of Anonymity," *GamePro*, 28 October 2010, http://www.gamepro.com/article/features/217085/the-psychology-of-anonymity.

22. Julie Zhuo, "Where Anonymity Breeds Contempt," *New York Times*, 29 November 2010, http://www.nytimes.com/2010/11/30/opinion/30zhuo.html?nl=todaysheadlines&emc=a212.

23. P. G. Zimbardo, "The Human Choice: Individuation, Reason, and Order versus Deindividuation, Impulse, and Chaos," in *Nebraska Symposium on Motivation,* eds. W. J. Arnold and D. Levine (Lincoln, NE: University of Nebraska Press, 1969), 237–307.

24. Emanuel Adler, "Complex Deterrence in the Asymmetric-Warfare Era," in *Complex Deterrence, Strategy in the Global Age,* eds. T. V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago, IL: University of Chicago Press, 2009), 85–104.

25. Tom Postmes and Russell Spears, "Deindividuation and Antinormative Behavior: A Meta-Analysis," *Psychological Bulletin* 123, no. 3 (May 1998): 238–59.

26. Zimbardo, “The Human Choice.” Zimbardo’s findings were supported by other studies which found that altered responsibility leads to increased antisocial behavior. These studies concluded “subjects were almost twice as aggressive if they did not feel responsible as were those who were made to feel responsible for their actions” According to the studies of Zimbardo, one of the leading researchers in the psychological field of deindividuation, individuals are more likely to carry out antisocial acts when they achieve a deindividuated state. In a 1969 study, Zimbardo used students to “administer” shocks to subjects in order to test his hypothesis. The experiments showed that individuals who achieved a deindividuated state appeared to act more aggressively than those who did not. Specifically his findings tended to suggest the combination of anonymity within a group dynamic increased aggressive behavior.

27. Leslie L. Downing and Robert D. Johnson, “Deindividuation and Valence of Cues: Effects on Prosocial and Antisocial Behavior,” *Journal of Personality and Social Psychology* 37, no. 9 (September 1979): 1,532–38.

28. Ibid.

29. Ibid.

30. Robert I. Watson, “Investigation into Deindividuation Using A Cross-Cultural Survey Technique,” *Journal of Personality and Social Psychology* 25, no. 3 (March 1973): 342–45.

31. Fox News, “Militants Behead American Hostage in Iraq,” *Fox News.com*, 11 May 2004, http://www.foxnews.com/story/0,2933,119615,00.html. In addition to the IRA, throughout the Middle East acts of terrorism and many attacks on civilians and military targets are marked by a common thread, the masking of the perpetrators identity. One of the most glaring acts of violence was the beheading of Nicolas Berg by Abu Musab al-Zarqawi in 2004. Zarqawi and his men beheaded Berg while taping the act, and did so with their identities masked by head coverings. Another example is the beheading of journalist Daniel Pearl in 2002.

32. A. P. Silke, “Deindividuation, Anonymity, and Violence: Findings from Northern Ireland,” *Journal of Social Psychology* 143, no. 4 (April 2003): 493–99.

33. Postmes and Spears, “Deindividuation and Antinormative Behavior,” 238–59.

34. While Kapur’s study is focused on nuclear threats, it is arguably applicable to a broader set of threats including biological, chemical, and cyber.

35. S. Paul Kapur, "Deterring Nuclear Terrorists," in *Complex Deterrence, Strategy in the Global Age*, ed. T. V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago, IL: University of Chicago Press, 2009) 109–25.

36. Ray Kurzweil, *The Singularity is Near: When Human Transcend Biology* (New York, NY: Viking Press, 2005). Small groups and individuals may become capable of producing weapons that previously were accessible only to financially successful nation-states. Even today, an ever-increasing level of scientific knowledge has allowed mankind to advance technology to amazing levels. Many technology advances are following along the basic theory of Moore's Law. What would have taken 100 years and the resources of a major nation-state to accomplish in the past, now takes approximately 25 years and the resources of a regional power. As technology continues to advance and individuals can access information that in the past was beyond their data gathering and economic resources, that 25-year time frame may be compressed into 14 years and then further into seven, while the investment required decreases to that which an individual or small group can afford.

37. Center for Strategy and Technology, "Blue Horizons IV: Deterrence in the Age of Surprise" (briefing, Air War College, Maxwell AFB, AL, 2010), 1–39.

38. Richard G. Hewlett and Oscar E. Anderson, Jr., *The New World: A History of the United States Atomic Energy Commission*, vol. 1, 1939/1946 (Oak Ridge, TN: US AEC Technical Information Center, 1972), 723–24. A case in point is the Manhattan Project undertaken by the United States to produce the first atomic weapon. A huge national effort was required to create the first atomic weapon in 1945. The United States invested $1.89 billion ($21.6 billion in 1996 constant dollars), built many research laboratories, and employed thousands of scientist and engineers to construct four weapons by 1945. This includes capital and operations costs from 1942 through 1945. Costs adjusted using a base year of 1944 (the year of highest Manhattan Project expenditures).

39. David E. Hoffman, *The Dead Hand: The Untold Story of the Cold War Arms Race and its Dangerous Legacy* (New York, NY: Random House, 2009), 101–03. Hoffman goes into great detail of the Soviet's secret development of genetically altered biological weapons against the prohibitions of the Biological and Toxin Weapons Convention. The Soviets were attempting to create a new generation of germs resistant to antibiotic under Projects Factor and Bonfire. Even today, the Russian government has never fully admitted to nor opened up its archives on the successful state run biological weapons program.

40. Pallotta and Finnin, "DIT Biology," 2–26; Michael Snyder, Jiang Du, and Mark Gerstein, "Personal Genome Sequencing: Current

Approaches and Challenges," *Genes and Development,* 1 November 2010, http://genesdev.cshlp.org/content/24/5/423.full; and Dr. Beth Perry (Los Alamos National Lab), interview by the author, 18 January 2010. For example, over the last 10 years an exponential increase in DNA knowledge and corresponding exponential decrease in the costs required, as well as the number of genomes sequenced, has allowed genetically altered biological weapon manufacturing to start its descent from the nation-state level to the individual. Basic genetic research and development can be broken into nine different levels. Ten years ago, work on any of the nine levels required an advanced degree (PhD) and the resources of a large laboratory. However, as of May 2010, the first three levels of genetic work can be done by an individual without a degree or specialized training, with equipment and instructions retrieved from the Internet or at a local store. In 10–15 years, graduate-level individuals will have the capability to create a new biological weapon. It is postulated that in 25 years all nine levels may be available to an individual with knowledge and equipment cheaply acquired from public sources that are difficult to trace. While the ability to make synthetic biological weapons currently still resides at the industrial level, the same advancements in technology that allow genetic research to be done by individuals and small groups are also beginning to allow individuals to work in the synthetic biology field. Where previously only scientists working for a

nation could create new weapons, technological advances over the next quarter century will more than likely give anonymous individuals or small groups the technological capability to develop/use the same weapons. Many predict that in 25 years, an individual or nonstate group may easily create a synthetic biological weapon to attack specific human characteristics within a population, creating a mass casualty event.

41. Michael A. Innes, "The Social Construction of Militant Sanctuary," research paper (London: Crisis State Research Center, London School of Economics & Political Science, 21 Oct 2009), 2–4, http://www.docstoc.com/docs/50526966/Innes-Militant-Sanctuary.

42. Hoffman, *The Dead Hand*, 126–42.

43. Benjamin Franklin, *Memoirs of the Life and Writings of Benjamin Franklin*, ed. William Franklin (Philadelphia, PA: T. S. Manning, 1818), 270; and Johnny Kilman and George Costello, eds., *The Constitution of the United States of America: Analysis and Interpretation*, GPO Access, 2008, 1,281–356, http://www.gpoaccess.gov/constitution/pdf2002/022.pdf. However a major impediment to the transparency initiative may well be the citizens of the country it is attempting to protect. This is especially true in democracies such as the United States. The feelings of many Americans are summed up by Benjamin Franklin when he wrote, "They who can give up essential liberty to obtain a little temporary safety, deserve

neither liberty nor safety". Much like the limited expectation to privacy when in public (US Constitution, Fourth Amendment), all electrons sent via the public domain may need to become part of the public record. Whatever level of transparency is achieved, it will not be 100 percent effective. Therefore the United States will also need to build a societal immunization system against attacks that will deny nonstate actors the capability and opportunity to launch attacks.

44. Kapur, "Deterring Nuclear Terrorists," 111–16, discusses effects of strategies designed to affect motivation, opportunity and capability.

45. Jerrold M. Post, *Mind of the Terrorist: The Psychology of Terrorism from the IRA to AL-Qaeda* (New York, NY: Palgrave Macmillan, 2007), 219–41, 254–56. Strategic communications capabilities are another part of creating a transparent system. Today's modern media proliferates scenes of violence and spreads stories with questionable facts around the world creating or magnifying grievances. A robust strategic communications program should focus on the reduction of grievances and the ideation that violence solves problems, making deterrence more likely to be successful.

46. Ibid., 254–56. Many studies of terrorism have discussed the fact that most individuals committing terrorist acts do care about family and have their own set of moral values. By influencing the social norms

of the groups individuals associate with the negative results from deindividuation may be nullified. In the case of families, terrorists need to be deterred from acting by understanding and believing that a nuclear or biological attack may be harmful to themselves or their families through radiation/fallout or the spread of infections throughout the world. At the same time some individuals, such as those following Islam, may be deterred by persuading them to look at different reading of the Koran that focus on the teachings against "mass casualties, including the killing of innocents, and the requirement to not poison the earth and living things."

47. Future MAP Program (futures markets applied to prediction), "A Market in the Future of the Middle East," http://www.iwar.org.uk/news-archive/tia/futuremap-program.htm; and Business Wire, "Singapore Develops Risk Assessment and Horizon Scanning (RAHS) System to Anticipate Future," *Allbusiness.com*, 1 March 2007, www.allbusiness.com/services/business.../4539437-1.html. Singapore is creating a transparent network of information used to identify potential nonstate threats through its risk assessment and horizon scanning (RAHS) algorithm. The RAHS attempts to detect weak signals and accomplish pattern analysis which can be applied to numerous areas to include prediction of terrorist attacks. This program appears to be similar to the aborted 2003 Department of Defense and

Defense Advanced Research Agency initiative. As a result of information garnered from a transparent information system, groups likely to act could be identified, communicated with, and deterred. By engaging these groups and influencing the mindset of the membership, the effects of deindividuation can be mitigated and thus attacks may not occur. In order to gather more data, the United States likewise needs to invest in technology capable of data storage, sensor capability and integration, and automatic threat assessment. Quantum computing may be required to bring all of these capabilities together on a global scale. This process may actually identify those likely to act or, through phishing, at least make them believe they have been discovered.

48. Many types of individuals using terrorism, even hardcore "terrorists," do not like to take operational risks and may be deterred by any uncertainty in their chances for success. See Jenkins and Davis, *Deterrence and Influence*, xi–xiii, for a more detailed discussion.

49. Snyder, *Deterrence and Defense*, 14–16.

50. Avery Plaw, *Targeting Terrorists: A License to Kill?* (Hampshire, UK: Ashgate Publishing Limited, 2008), 173–76.

51. Ibid., 165–97.

52. David Kilcullen, *Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (New York, NY: Oxford University Press, 2009), 263–89.

53. Ibid.

54. Dr. Kim (Bell Laboratories), interview by the author, 28 January 2011.

55. Center for Strategy and Technology, “Blue Horizons IV,” 38.

56. Ibid.