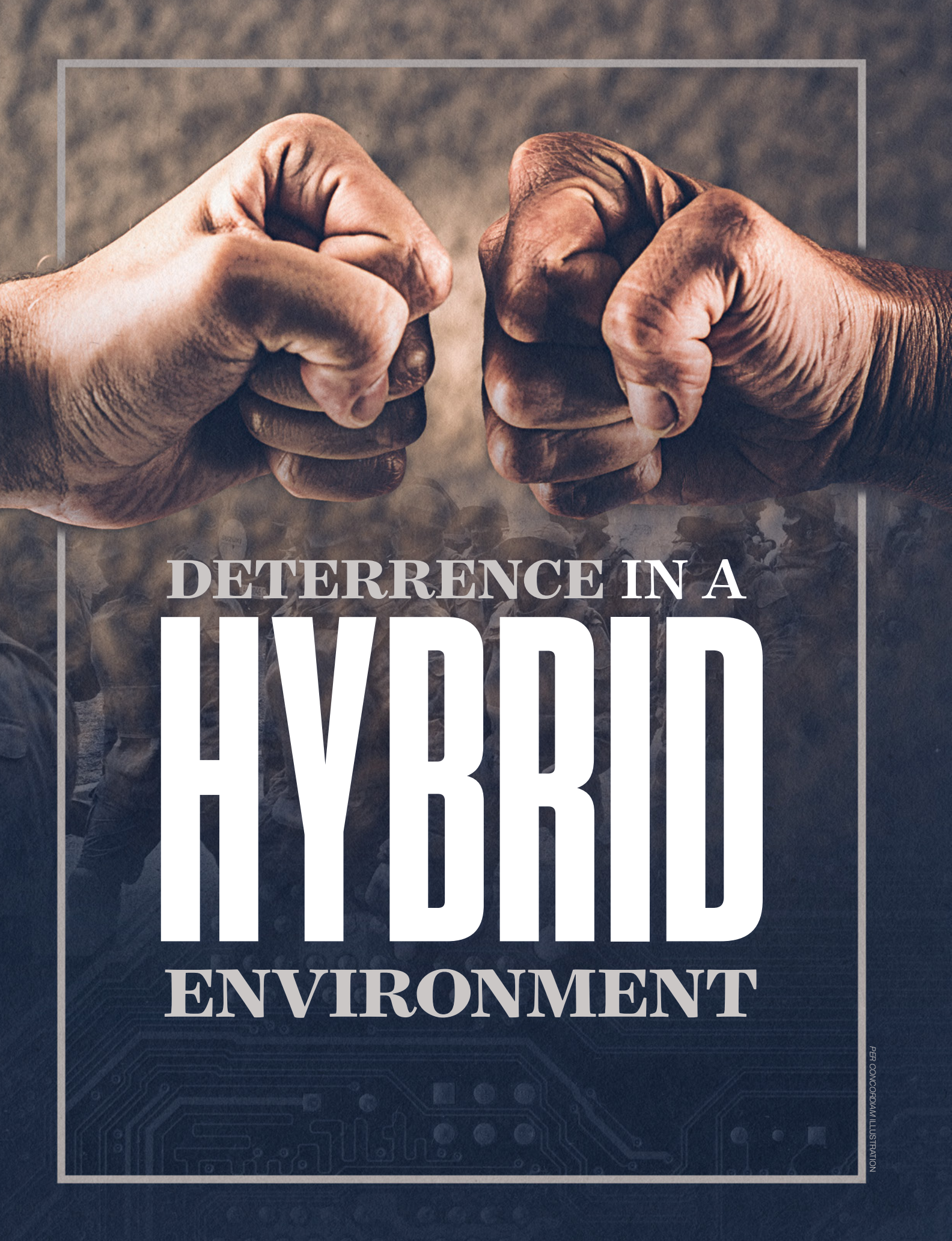


DETERRENCE IN A HYBRID ENVIRONMENT

PER CONCORDIAM ILLUSTRATION

Defending against nonlinear threats

By **Col. John J. Neal**, U.S. Army

Cold War deterrence theories are no longer sufficient to guide states in the current era of great power competition. The linear concept of military escalation is not valid in an environment where nonmilitary means are the tools of choice for aggressors to advance their strategic goals. Activities categorized as below the level of armed conflict now pose a significant threat to national security, potentially on par with military threats. States are also more willing to use nonmilitary means because of the inherent ambiguity and lack of behavioral norms associated with the use of these tools. Therefore, governments must revise the way they think about deterrence to take these changes into account and develop effective strategies that can better address national security concerns.

The inherent ambiguity in the current security environment is reflected in the lack of distinction between military and nonmilitary means. The military tools available to the state have been greatly expanded. These have traditionally included land, air and maritime formations and the capabilities designed to inflict lethal harm on an adversary, which is how they are defined for the purposes of this article. However, state armed forces now often control some means not usually associated with the military, such as cyber, information and economic tools. This lack of distinction between military and nonmilitary means further complicates deterrence in the current environment.

Deterrence concepts developed during the Cold War focused primarily on the use of military means based on a clear correlation of forces that indicated the probability of success. Escalation along a commonly understood scale played a key role. These ideas were applied to deterrence by denial and by punishment strategies to protect national interests. In addition, deterrence thinking yielded key framing questions, identified basic requirements and recognized that adversaries would take an incremental approach to undermine deterrence efforts. These ideas were valid in a world where military tools were the primary means of aggression.

Policymakers have turned to a combination of Cold War and emerging deterrence theories to address the confrontational behavior of Russia and China over the past two decades. In doing so, they have not sufficiently accounted for the differences between the Cold War and the current environment. There are still significant shortfalls in deterrence thinking that need to be addressed. First, the central role of military force and the linear nature of conflict are no longer applicable. These ideas should be replaced by an understanding of the parity of military and nonmilitary means to threaten national interests. In addition, the Cold War concepts of basic deterrence requirements, key framing questions, and the adversaries' incremental approach are still valid, but these ideas have new meaning in the context of nonmilitary means.

Changes in the environment

There are three nonmilitary areas in particular that are greater threats than they were several decades ago: cyber, information warfare and economic. These tools also have different employment-time considerations than military means. Each poses similar challenges of response and scale that complicate the formulation of deterrence strategies.

Blasts from NATO's Exercise Trident Juncture 18, off the coast of Trondheim, Norway, send up water geysers. Such exercises deter aggression by demonstrating NATO's capability and resolve. REUTERS

The cyber threat is of particular concern. Cyber tools can be used to support military, economic and information warfare operations, or they can be used to surveil, damage or destroy systems in the cyber domain. There are numerous examples of these actions committed by state actors. Andy Greenberg noted in a *Wired* magazine article that the Russian "NotPetya" cyber attack against Ukraine in 2017 caused more than $10 billion of damage worldwide. In 2011, a group of hackers based in North Korea — presumably affiliated with that government — attacked Sony Pictures' networks for producing a movie satirizing North Korean leader Kim Jong Un. According to a study

by the Foundation for Defense of Democracies, Chinese cyber incursions and network exploitations have caused significant damage to foreign companies. Despite numerous confirmed attacks by state actors, there is still no consensus on where these actions fit in the spectrum of conflict.

While the use of information against adversaries is millennia old, it became much more prevalent with the advent of digital mass media and the internet. Some states take a broad and less constrained approach to information warfare. In a 2011 conceptual document on activities in the information space, the Russian Defense Ministry described information warfare as carrying out psychological campaigns against a state's population to destabilize both the society and the government. Russian information warfare has increased capacity and access over the past two decades through wider media presence, social networks and cyber tools. These changes have significantly increased information warfare's potential to threaten national security.

As with information warfare, economic tools have been used for centuries to influence other states, but the increased interconnectedness of globalization, coupled with economic digital vulnerabilities, means that it poses a greater threat than in the past. There is strong evidence to suggest that Russia uses economic tools to manipulate other states and advance its national interests. A 2016 Center for Strategic and International Studies report finds a correlation between the level of Russia's economic presence in a country and the deterioration of democratic values and standards. Similarly, Chinese theft of business intelligence and intellectual property is used to increase the competitiveness of Chinese businesses while negatively affecting companies outside China, as highlighted in a MindPoint Group white paper from 2014. Economic means are also ambiguous in terms of how they fit in the spectrum of conflict because while some economic behaviors such as tariffs are well understood in escalation, others such as economic influence are not.

An overarching issue is how nonmilitary means change the nature of time and tempo in conflict. In military conflict, there is typically a distinct initiation of hostilities, usually through the overt use of lethal force, preceded by a buildup, which may offer a warning of impending aggression. Nonmilitary means have very different timelines for execution and effect. Information operations take months or even years to produce effects. Conversely, cyber tools can cause catastrophic effects in a matter of minutes, potentially with no warning. These widely varying chronological factors must be accounted for in developing future approaches to deterrence.

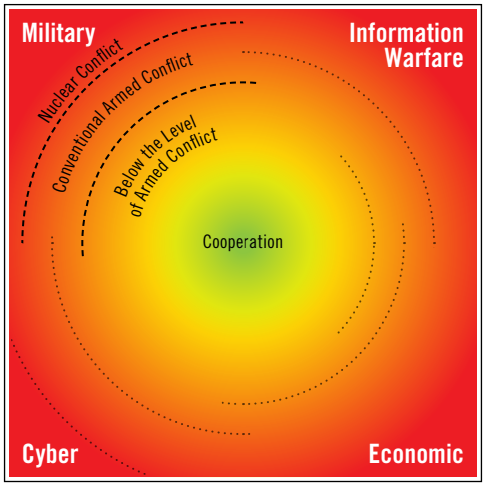
U.S. Marines with the 24th Marine Expeditionary Unit hike to a cold-weather training site in Iceland during NATO's Exercise Trident Juncture 18. REUTERS

Table 1. **Nonlinear Deterrence**

Understand the Environment

1. Know the adversary.
2. Recognize the increased threat nonmilitary means pose to national security.
3. Lower the threshold for the use of nonmilitary means.
4. Know the adversary's incremental approach.
5. Recognize the indistinctness of peace and war.

Visualize the Environment



Deterrent Approaches

1. Reduce ambiguity.
2. Go beyond domain-limited actions.
3. Apply key aspects of deterrence theory:
   - Decide who, what and when to deter, and what is worth deterring.
   - Identify the aggressor; clearly signal the aggressor; possess the capability to respond.
   - Deter by punishment.

Source: Col. John J. Neal, U.S. Army

Deterrence theory

There are several aspects of military deterrence that must be reassessed to create future deterrence policy. First, in military deterrence the spectrum of conflict is viewed as linear, where the use of force occurs along a known scale. Secondly, this scale infers that the use and effects of specific military tools are widely understood. This understanding is reinforced by a competitor's assessment of the correlation of forces, which typically focuses on military capabilities. Finally, military deterrence theory does not account for the effects of nonmilitary tools in waging war.

The linear spectrum of conflict is one of the best-known legacies of the Cold War. In 1965, theorist Herman Kahn used a ladder metaphor to frame escalation. This consists of a linear arrangement of crisis levels, with associated levels of risk. Actors ascend or descend the ladder by conducting actions that correspondingly increase or decrease the opponent's threat level. The concept had applications for Cold War scenarios and, in particular, conflict between the U.S. and the Soviet Union.

The correlation-of-forces method used to determine the costs of a given action is greatly facilitated by the relative ease with which each state can quantitatively measure their respective strengths and weaknesses. However, nonmilitary tools do not lend themselves to this kind of quantitative examination, so the potential impact of the use of these tools is much more abstract. There is also a commonly accepted framework of the potential costs and reactions to military escalation. The same cannot be said of the nonmilitary means. All of this complicates the calculation of the deterrent effect of nonmilitary tools.

Though there are bodies of literature on the use of military, cyber, information and economic tools, each area is often treated in isolation when addressing deterrence. Deterrence thinking tends to focus on symmetrical domain or area responses, such as a military reaction to a military provocation, without viewing these activities in the larger context of the competitor's behavior and intent. A fully integrated, multidomain approach to deterrence that recognizes the changing nature of conflict is required to shape effective deterrence policy.

State-versus-state deterrence

For a theory to be useful to practitioners, it must provide a consistent way of approaching a complex problem with multiple factors and variables. Changes in the security environment, including the interdependent use of military and nonmilitary means along widely varying timelines where competitors seek to exploit ambiguity and nonattribution, have made deterrence inherently more complex. Existing deterrence theory and associated scholarship do not adequately address these changes. I propose the idea of "nonlinear deterrence" to describe an updated concept that accounts for these changing conditions. Nonlinear deterrence is composed of three elements. The first, understanding the environment, is composed of five principles that account for adversary behavior, emerging tools, and the effect both have on the concepts of peace and war. The second part is visualizing the environment. Table 1 (above) depicts the interaction of military and nonmilitary means with relative risks to national security. The third part of the concept is deterrent approaches; practical applications to drive deterrence policy development in the future.

Understand the environment

The first component of nonlinear deterrence is understanding the environment. It consists of five principles, which are an amalgamation of emerging scholarship that includes Michael Mazarr's seven hypotheses of the gray zone (aggression that is coercive but below the threshold of conventional military conflict); traditional thinking on deterrence from theorists like Lawrence Freedman, John Mearsheimer, Alexander George and Richard Smoke; and ideas gleaned from trends in the environment. The first principle is understanding the aggressor. Theorist André Beaufre put it succinctly when

he wrote that "deterrence must therefore be played with the enemy's doctrines as a yardstick." Both Russia and China have published concepts of modern warfare that embrace the use of nonmilitary means. Russian military theorists first put forth their idea of "new generation" warfare in 2013 in the journal *Military Thought*. The authors, S.G. Chekinov and S.A. Bogdanov, described a concept that involves the combined use of nonmilitary and military tools to target the adversary's armed forces and its population. In fact, Russian theorists have advanced the idea that nonmilitary means could be the predominate factor in determining the outcome of hostilities.

The Cold War-era U.S. listening station Field Station Berlin is no longer used. Technology has advanced, but the need to monitor Russian activity remains.
AFP/GETTY IMAGES

The second principle in understanding the environment is recognizing the increased threat nonmilitary means pose to national security. As with the first principle, this is clearly a concept that some states embrace. There are numerous examples of how cyber, information warfare and economic means have been used to cripple other states. These tools currently pose a threat to national security on par with military means. In addition, they do not have the geographic limitations or timelines associated with military tools, requiring a different understanding of their applications.

The third principle is the greater willingness to use nonmilitary rather than military means. This is in part why some countries apply these tools to support the methods described in the first principle. Nonmilitary actions, particularly in cyber and information warfare, are difficult to attribute, freeing states to use them with less risk of punishment. There are far fewer treaties, agreements and laws, if any, that govern the use of nonmilitary tools, so there is less of a codified basis for retaliation. Furthermore, there are no established scales of behavior that define the severity of specific nonmilitary actions. All of these assist countries in advancing their goals.

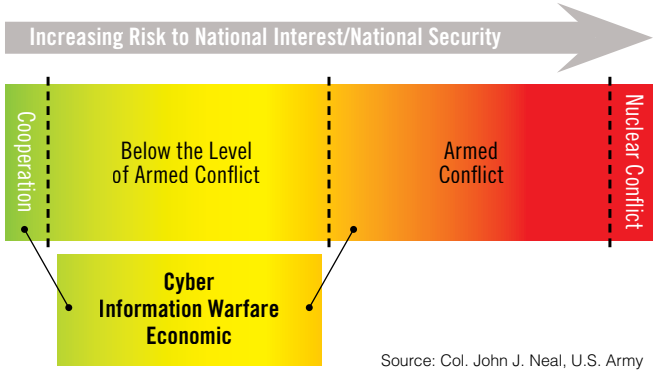
The fourth principle is recognizing that some states take an incremental approach, using a series of small actions to achieve long-term ends and avoid overt conflict. Thomas Schelling termed this concept "salami-slicing" during the Cold War and it has been further described as "gradualism" by Mazarr. In this process, a state conducts a series of activities that in and of themselves do not escalate the level of tension between states. However, collectively these actions create a new status quo advantageous to the aggressor. This approach necessitates an interconnected view of military and nonmilitary actions over time to understand the broader context and intent.

The fifth principle is to stop thinking strictly in terms of peace and war. Instead, it should be recognized that the line between the two has been blurred to the point that they are no longer distinct. This state of affairs puts governments at a disadvantage since they traditionally think in binary terms and compartmentalize their tools. Conversely, this condition, described by Lucas Kello as "unpeace" in his book *The Virtual Weapon*, favors the aggressor, allowing them to maximize the use of nonmilitary means and exploit the incremental approach.

Visualize the environment

The second part of nonlinear deterrence is visualizing the environment. The ability to see and understand the connections between the use of military and nonmilitary tools over time is crucial to recognizing how adversary activities threaten national interests. It facilitates the development of coherent policies and actions to deter further aggression and to anticipate possible areas of concern. To present the nonlinear visual model, it is necessary to review past, current and evolving graphic depictions of the spectrum of conflict and where the various means fit into them.

Figure 1. **Linear Spectrum of Conflict Focused on Military Means**



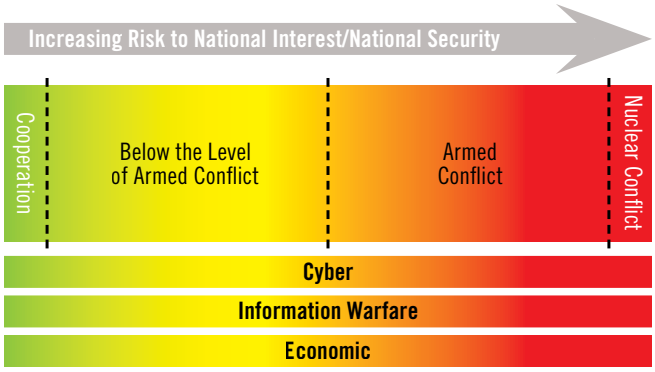
Source: Col. John J. Neal, U.S. Army

Past concepts have taken the form of a sliding scale, which focused on the use of military force with nonmilitary means being a complementary aspect of military tools (see Figure 1, above). This reflected the idea that military actions have a well-defined escalatory hierarchy with clear distinctions and that nonmilitary means have an ill-defined supporting role and only pose a marginal threat.

We now recognize that nonmilitary means pose greater levels of threat to national security, potentially on par with military means. However, these areas are often viewed in isolation, with a potential theoretical scale of escalation

applied (see Figure 2, below). This reflects the current focus on domain-specific deterrence without accounting for how actions in each of these areas contribute to a deteriorating security environment.

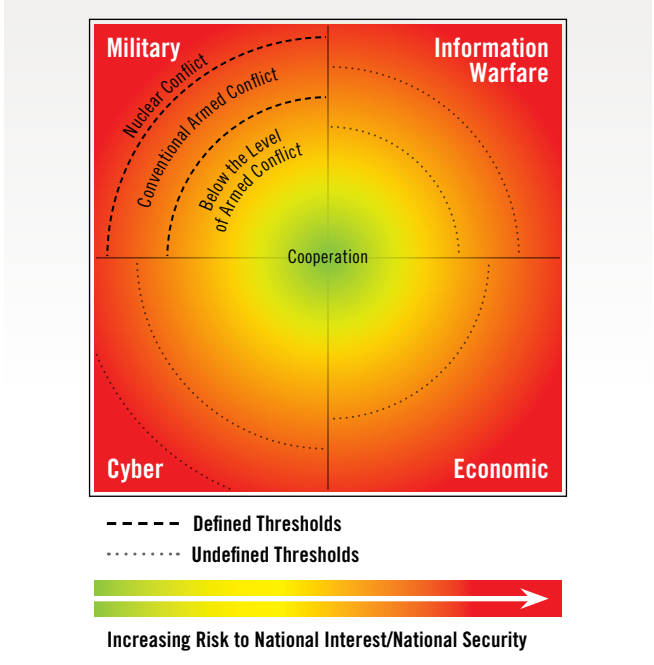
Figure 2. **Spectrum with Parity of Military and Nonmilitary**



Source: Col. John J. Neal, U.S. Army

The evolving concept model moves away from the escalation ladder, since it is less relevant as competitors seek ways to circumvent established norms. In this model, military and nonmilitary means are represented as having equality in their threat to national interests and national security. The thresholds for the use of military force are demarcated, and the potential for thresholds in the nonmilitary means are also accounted for, should they be defined (see Figure 3, below).

Figure 3. **Multivector Spectrum of Conflict**



Source: Col. John J. Neal, U.S. Army

However, the military and nonmilitary categories cannot be viewed in isolation. The quadrant lines in this model reflect the idea that each area is distinct and separate, which is the same concept portrayed in Figure 2 using parallel lines.

The nonlinear deterrence visualization of the environment combines the idea of threat parity among military and nonmilitary means, the interdependence of these means, and the aggregate increased risk to national interests and national security. This model is designed to highlight how actions in one area are connected to activities in another, such as the use of military force to create an economic effect. This model also shows how potential thresholds may be applicable in more than one area. To illustrate these concepts, actions in and around Ukraine from April to November 2018 are displayed. It shows how activities in multiple areas are connected and how they push the limits of acceptable behavior (see Figure 4, following page). This example depicts a state operating in a specific geographic area acting against another state. The model can be expanded to a state acting across the globe over a longer period of time or contracted to a smaller area and a shorter period in order to draw out connections and risks.

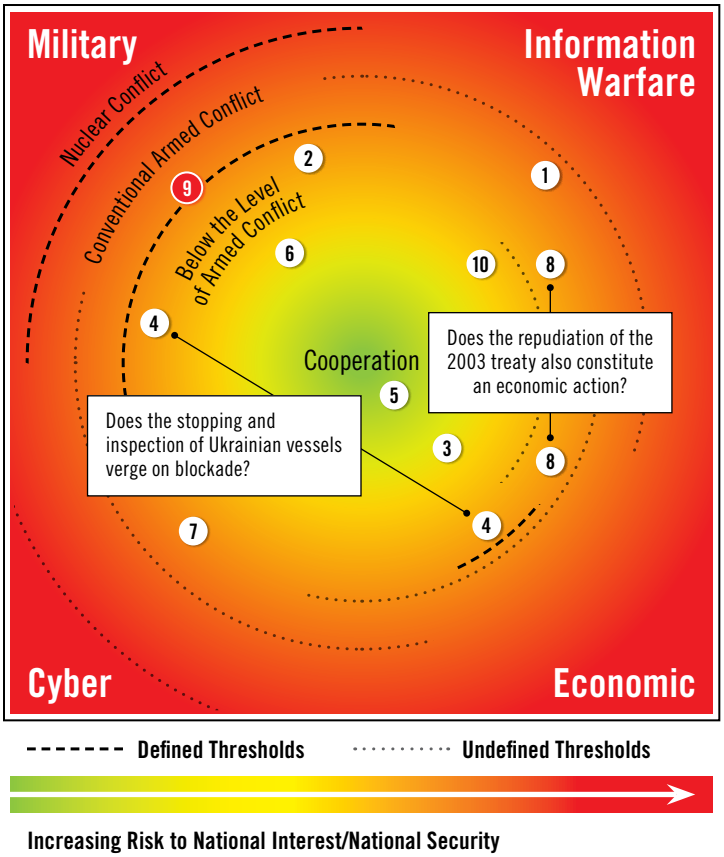
Visualization of the environment is a key element of the nonlinear deterrence concept. It incorporates and characterizes the principles of "understanding the environment" in a graphic display that sets the conditions for the application of the "deterrent approaches" principles. The model is also adaptive. It is designed so that it can incorporate emerging deterrence concepts and terminology to account for the changing nature of conflict and the role that various tools play in the environment.

Deterrent approaches

The first principle of deterrent approaches is reducing ambiguity. Ambiguity is a critical enabler of competitor strategies. Decreasing it will significantly degrade an aggressor's ability to achieve its goals. Doing so involves establishing defined parameters and norms of behavior and challenging adversaries when they violate them. As described by Thomas Schelling in *The Strategy of Conflict*, when disrupting an incremental threat, disrupting individual acts is more effective than countering the overall objective. Using this method, states can incrementally hinder adversaries before conditions irrevocably change in the adversary's favor.

One way to define parameters is to establish clear red lines for actions that threaten national interests. In doing so, states can definitively challenge adversary behavior. Red lines are defined as the stated position of an entity that it will act if another violates that position. One example is Article 5 of the North Atlantic Treaty, which states that an armed attack against one member of the Alliance will be answered by all. However, there are inherent vulnerabilities in red lines. David Altman noted in "Red Lines and Faits Accomplis in Interstate Coercion and Crisis" that red lines are arbitrary and can be imprecise, incomplete and unverifiable. NATO's Article 5 illustrates some of these vulnerabilities. In 2014, NATO members agreed that a cyber attack met the criteria for an Article 5 violation. This step made sense, given the

Figure 4. Nonlinear Visualization of the Environment



Actions in and around Ukraine
(April-November 2018)

1. **2018:** Russian disinformation campaign claims: Ukraine infected sea with cholera, Ukraine attempted to smuggle a nuclear bomb into Crimea, Ukraine naval base is for NATO.
2. **April-November:** Russian buildup of land and maritime units in Crimea/Sea of Azov.
3. **May:** Russia opens Kerch Bridge leading to a loss of Ukraine freight traffic.
4. **May-October:** Russia stops and inspects merchant ships bound for Ukraine ports in Sea of Azov.
5. **September:** Russia states it complies with 2003 treaty that Kerch Strait is both Ukraine and Russia.
6. **October:** Russian joint maritime/land exercises in Crimea, Black Sea.
7. **October-November:** Russian cyber data collection and attacks on Ukraine government in conjunction with Russian Kerch Strait operations.
8. **November 15-21:** Russia declares it has complete sovereignty over Kerch Strait; United Nations Convention on the Law of the Sea not applicable.
9. **November 23-26:** Russia attacks three Ukrainian ships and captures Ukrainian sailors while transiting the Kerch Strait.
10. **November 26:** TASS reports Ukrainian ships violated Russian border.

Source: Col. John J. Neal, U.S. Army

increased cyber threat, but it highlights some of the red line vulnerabilities. However, this position is both imprecise and incomplete, since the Alliance has not clearly defined what constitutes a cyber attack. It is also difficult to verify, since one of the advantages to cyber is its inherent deniability. Finally, in the years since NATO took this position there have been multiple cyber attacks on its members with no clear retaliation and no declaration of Article 5. To be effective, red lines must be clearly defined, backed by a credible threat and, most importantly, they must be enforced.

Another method is establishing the legal framework for accepted behavior through treaties, international agreements and national policy. One of the fundamental issues with nonmilitary means is the lack of such a framework, enabling adversaries to exploit these means to great effect. The idea of a treaty that governs cyber activity is not new. National governments, international organizations and private corporations have all called for a digital Geneva Convention that would govern the use of cyber tools. This raises several issues. One is the difficulty in getting powerful competitors to agree on meaningful standards, particularly since it is in the interest of many of them not to do so. Another is that some states will not adhere to the treaty to which they agreed. Finally, since one of the major issues with nonmilitary means is attribution, verifying treaty violations will be difficult. Even with these drawbacks, it is still advantageous to work to establish these agreements. In addition, states can create their own standards of behavior and thresholds for retaliation in order to reduce ambiguity. This may be an effort to define an escalation hierarchy similar to the escalation ladder of military actions.

The second principle of deterrent approaches is going beyond domain-limited actions. In many cases, states respond or posture in the same domain where the aggressor is operating. For example, the U.S. is taking a stronger position in opposing cyber threats by expanding operations in cyberspace. NATO has enlarged its military force posture and activities in response to increased military aggression by Russia. To be more effective, states need to develop a codified strategy that integrates the use of tools across multiple domains to precisely target aggressor actions.

The third principle of deterrent approaches is accounting for key aspects of deterrence theory. The foremost of these aspects is deciding who, what and when to deter, and, fundamentally, what is worth deterring. These requirements establish the foundation for a deterrence strategy and allow policymakers to examine threats in the context of national interests in order to prioritize efforts and resources in a coherent manner.

The three requirements for deterrence, described by Schelling in *Arms and Influence*, are also applicable in the current environment. The first is attribution; the state can unmistakably identify the aggressor. The second is signaling;

A member of the Swedish Army's Gotland regiment positions a machine gun as part of a live-fire exercise on the island of Gotland in February 2019. After the annexation of Crimea, the conflict in Ukraine, incidents of Russian military jets approaching Swedish aircraft, and the 2014 sighting near Stockholm of a mystery submarine suspected to be Russian, Sweden has scrambled to beef up a military that was cut back after the end of the Cold War. AFP/GETTY IMAGES

the state clearly conveys its messages to the aggressor. The third is credibility; the state possesses a viable capability that it will actually use. Each of these requirements are challenging in the context of nonmilitary means. Cyber and information warfare work optimally when they are unattributable. Even economic means, which are usually overt, may be ambiguous as to their true intent. Furthermore, revealing capabilities in nonmilitary areas to convey credibility will often result in the reduction of those capabilities since countermeasures can be rapidly developed.

The next aspect is the balance between deterrence by denial and deterrence by punishment. Both are valid methods, but deterrence by punishment is often a more viable way of deterring the use of nonmilitary means. There are several reasons for this. First, it is very difficult to deny competitors the conditions that enable attacks. Many countries are premised on free and open societies, with their inherent unrestricted access to cyberspace and media. To limit these freedoms would go against these principles. Second, the defenses against nonmilitary aggression are not effective to the point that they can deny an attacker the ability to attain its goals. Third, it is difficult to deny aggressors access to nonmilitary means since these tools are often cheap, prolific and dual-use. As conditions change and technologies advance, there may be a shift back to deterrence by denial, but for the time being punishment offers more deterrence potential.

The concepts of counterforce and countervalue targeting have applications in deterrence by punishment. These methods allow for the nuanced use of nonmilitary tools to impose costs on adversaries. Max Smeets recently described this concept for the use of cyber tools in his paper, "The Strategic Promise of Offensive Cyber Operations." He points out that this approach has already been used in multiple instances, even if the applications have not been labeled as such. This same approach can be applied to economic tools, where some actions may target a specific capability while others are focused on broader areas.

Conclusion

The nature of conflict is changing. States are increasingly turning to nonmilitary means to advance their goals, altering the concept of escalation in the process. The interdependent use of military and nonmilitary means has blurred the lines between peace and war. These factors have created conditions in which competitors exploit the ambiguity of their actions and the lack of international norms of behavior to threaten other states in ways not previously anticipated. To secure their interests in the future, states must adapt their understanding of deterrence.

Nonlinear deterrence offers a way of thinking about deterrence that can assist in addressing the current security environment. It is an amalgamation of past and current thinking and of ideas drawn from recent competitor doctrine and behavior. It is also a departure point for further discussion and additional work in the development of state-versus-state deterrence that can be applied to national policy formulation. □