

COUNCIL *on* FOREIGN RELATIONS

Center for Preventive Action

58 East 68th Street, New York, New York 10065
tel 212.434.9400 fax 212.434.9800 www.cfr.org

Preventive Force and U.S. Foreign Policy

Workshop in Washington, DC

April 14, 2011

This workshop was made possible by the generosity of the Carnegie Corporation of New York.

Nine years ago, the George W. Bush administration explicitly articulated the U.S. right to “act preemptively” to forestall or prevent hostile acts by adversaries. Today, the Obama administration has retained the right to use preventive force, though under more limited circumstances, as spelled out in the 2010 National Security Strategy, in statements by government officials, and in practice in Pakistan, Yemen, Somalia, and—most notably—Libya.

In April 2011, the Center for Preventive Action at the Council on Foreign Relations convened a workshop in Washington, DC, to discuss “Preventive Force and U.S. Foreign Policy.” The workshop brought together experts from the U.S. government, think tanks, and academia to explore and assess the role of preventive force in U.S. foreign policy today and into the future. What follows is a summary of the discussion, which was conducted on a not-for-attribution basis.

Defining Preventive Force

At the outset of the workshop, participants attempted to define “preventive force”—a challenging task because discussion of preventive force is often imprecise or, according to one speaker, characterized by “lots of sloppy thinking.”

Preventive force is defined by the imminence of the threat to which it responds. As distilled by one participant, “preventive force is the use of forceful measures to avert a national security threat from materializing or evolving in a way that it poses a threat to materialize at a later stage. The imperative to use preventive force arises from the perceived cost of delay: it is better to act now than later.”

In this sense, preventive force is distinct from preemptive force—a concept with which it is often conflated. As one speaker pointed out, “preemption is something you do to forestall immediate attack—like the Israelis in 1967—whereas preventive force is preventing something farther into the future, such as preventing a future threat from emerging.” Another participant supported this distinction by posing a temporal test: only if a threat is instantaneous, overwhelming, and provides no moment for deliberation would the response be preemptive.

Of course, imminence is a subjective and flexible standard. Several participants questioned how a government can reliably establish imminence—in other words, what quality of intelligence or

knowledge is necessary to justify use of preventive force? Another speaker questioned whether imminence can remain a relevant heuristic when the United States exists in a “constant state of imminence”—for example, it is easy to imagine a terrorist group in a variety of locations with the capability to deliver a mass casualty attack at short notice.

In clarifying the concept of preventive force, participants also debated the meaning of “force.” As new technical capacities develop—particularly in cyberspace—the line between force and other types of coercion is blurring. Particularly with cyber capabilities, actors can now achieve kinetic effects for which military force used to be necessary. For this reason, the kinetic effects of an action may be the best way to classify it as force. Not all participants agreed, however, that cyber attacks like the Stuxnet virus that hobbled the Iranian nuclear program should constitute force. One participant suggested that the actor conducting the operation determines whether it constitutes force: if an operation—be it a naval quarantine or a cyber attack—is conducted by the military, employment of martial resources makes it a “use of force.” The effect of a more expansive definition of force, however, is that there are greater legal limitations under international laws governing the use of force.

Legality of Preventive Force

The legal questions surrounding preventive force are inextricable from the definitional issues outlined above. Under the United Nations (UN) Charter, states agreed to refrain from the use of force against other member states; the charter permits use of force only by the UN through Chapter VII Security Council authorization and in self-defense responding to an armed attack. Under this framework, preemption is illegal as is anticipatory self-defense.

Changes since 1945 have problematized the charter’s paradigm, however. In a world with weapons of mass destruction, states cannot respond to attacks post facto. As one speaker pointed out, “states do not have to wait until a missile is above their territory in the nuclear age.” The terrorist threat also makes anticipatory self-defense more necessary. As a result, in 2005, the UN secretary-general recognized the right to use force in anticipatory self-defense. Hence, preemption but not prevention is now considered to be permissible under international law.

In considering the legality of preemption, participants discussed the George W. Bush administration’s preemption doctrine, as articulated in the 2002 National Security Strategy, and the subsequent war in Iraq. According to one speaker, the Bush doctrine was not novel; rather, it adapted the concept of imminence to today’s threats and adversaries. The Bush administration understood preemption as acceptable only in particular cases and only when other means, including diplomacy, had already been exhausted. Although the Iraq war is often cited as an example of the Bush administration’s preemption doctrine, legally the Bush administration claimed to be acting under prior UN Security Council resolutions, not a theory of preemption. Nevertheless, legality is not tantamount to legitimacy: the political justification for the Iraq war (stopping Iraqi development of weapons of mass destruction) was different than the legal justification, and the political justification turned out to have little foundation.

Recent legal debates over preventive force have focused on the Bush and Obama administrations’ use of unmanned drones to target terrorists and insurgents. The State Department’s legal adviser, Harold Koh, has defended the legality of drones on two bases: first, as an act of self-defense under international law, and, second, as a necessary measure in the United States’ armed conflict with al-Qaeda. These are two completely different legal theories; only under the former justification are drones an example of preventive force and hence subject to an imminence standard.

Can Preventive Force Be Effective?

While preventive force is often ineffective, participants agreed that there are conditions under which it can succeed. According to one speaker, “Preventive force can be effective only if you successfully convey the degree of your commitment and if that commitment is adequate to solving the problem.” Most of the time, however, preventive force doesn’t work because policymakers default to limited force due to limited national interests or the perception that the cost of pursuing those interests is too high. Limited force then translates to limited effectiveness as adversaries probe the U.S. commitment and find that the United States has inadequate resolve to achieve its objectives. As one participant stated, “using limited means conveys you can afford to fail.”

Policymakers can mitigate the effectiveness dilemma in one of two ways: first, by successfully convincing the adversary that the U.S. level of commitment is higher than it actually is; or, second, if preventive force is a genuine signal that more decisive force will follow.

Evolving Missions for Preventive Force

As technology and international norms evolve, new preventive missions are emerging. Workshop participants saw a clear role for preventive force in counterterrorism, counterproliferation, operations in space, and cyber war. One speaker suggested a more expansive landscape of preventive missions, including civilian protection, humanitarian operations, organized crime, governance missions, environmental threats, global pandemics, and migration control. Overall, greater operational opportunities for preventive force are created by technological advances in precision strike, targeting, munitions, and real-time surveillance. Politically and normatively, preventive force is given more latitude with regard to counterterrorism, counter-WMD missions, and humanitarian operations. Certain constraints have also emerged, however; namely, a greater legitimacy imperative, growing intolerance for error in military operations, growing transparency about military operations and their effects (with the exception of cyber), the need to conduct operations in conjunction with other states, and the need to ensure that any operation is joint within the national command structure.

Discussion at the workshop focused primarily on cyber war. Cyberattacks can take many forms, but they are best for operations with advance time to plan and gather intelligence, ideally for use prior to or early in a kinetic conflict. Possible goals for cyberattacks include: disruption of weapons of mass destruction or missile production and research and development; early military action, like disruption of C2, air defenses, or troop deployments; compromising senior military personnel; covert action for regime change, as by tampering with electronic voting machines; financial attacks to drain treasuries; financial attacks to steal personal fortunes of adversary leaders; and attacks to undermine manufacturing capacity, power production, banking, and public confidence.

Two factors differentiate cyber from other types of preventive force. First, cyberattacks present an attribution problem: there is no reliable way to identify with absolute certainty the source of cyberattacks, creating opportunities for anonymous operations or misattribution. Second, cyberspace is an offense-dominated environment; currently, states are much better at offense than defense or deterrence, creating an imperative for first strike. Problematically, according to one speaker, there has been insufficient discussion of the virtues and drawbacks of offensive cyberattacks.

Workshop participants discussed the possibility of international agreements to mitigate the potential damage of a cyber war. One speaker proposed that states might agree to a cyber norm against targeting critical systems and infrastructure. Whereas some participants saw the Geneva Conventions

as a possible model for an international agreement on cyber, others disagreed because the Geneva Conventions pertain to targets that are not of military advantage. Instead, one participant suggested, the model should be nuclear arms control, where there is a strategic advantage to be gained but states decide that “on balance it is too terrifying for either side to enjoy certain capabilities.” Others took issue with the nuclear arms control models because there is no verification mechanism in cyberspace; instead they suggested that the “work most relevant to cyber is in the biological sphere,” where verification is equally difficult.