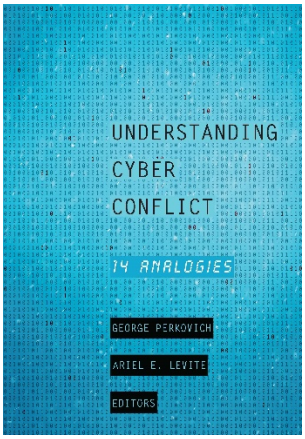

An Ounce of (Virtual) Prevention?

John Arquilla

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



6 An Ounce of (Virtual) Prevention?

JOHN ARQUILLA

Among the most paradoxical, clouded concepts in military and security affairs are the twin notions of "preventive war" and "preventive use of force." The former is commonly associated with starting a war at a most opportune moment—for example, while the prospects of defeating an enemy's military, seizing territory, or toppling a regime are good—or at least before a growing threat worsens. The latter reflects more modest ambition and consists of shorter, sharper actions aimed at avoiding more protracted conflict or at mitigating a dangerous situation.[1] Simply put, preventive war is about fighting now, not later, and for grander aims; preventive force is about using violence now in the hope of avoiding a full-blown war or to keep the strategic situation in an ongoing confrontation from deteriorating.

Preventive war, on the one hand, has a very long pedigree. Thucydides noted that the Spartans decided to wage war against Athens, amid crises over the smaller city-states of Corcyra and Potidaea, because "they feared the growth of the power of the Athenians, seeing most of Hellas already subject to them."[2] For more than two millennia since, decisions to go to war have often been made in fear of such growing power and of the potentially dire consequences of delaying a fight until a later time.

Yet it must be noted as well that adventurer-conquerors, such as Napoleon and Hitler, have also relied on notions of preventive war to rationalize blatant acts of aggression. Indeed, both men employed the logic of preventive war in their decisions to invade Russia. Thus, the preventive warfare concept can be nebulous—resorted to either out of fear or covetousness—and clearly has been subject to abuse.

Moral philosophers, therefore, have generally disapproved of preventive war.[3] So, too, did President Dwight D. Eisenhower, who in an important speech in 1954 categorically ruled out the idea of using the nuclear supremacy the United States then enjoyed to wage preventive war against Russia or China.[4]

Preventive force, on the other hand, is not fundamentally about trying to start a fight at the most opportune moment. Rather, it is a strategic construct designed for using a modicum of violence to thwart the rise of a fresh danger, to keep an ongoing conflict from widening, or, perhaps most important, to avoid

the outbreak of a large-scale conflict. A well-known example of the last motive is the Israeli air raid mounted against the Iraqi nuclear weapons facility at Osirak in 1981. This raid was a classic preventive act of violence, short in duration and applied quite sharply. In this instance it seems clear that the Israeli attack set back Saddam Hussein's plans to acquire a nuclear weapons capability, though it did not end his ambitions. Still, the "underground" nature of Saddam's reconstituted nuclear program moved slowly, guaranteeing that he would not have an ability to threaten mass destruction to deter the US-led Coalition that ejected Iraqi forces from Kuwait a decade later in 1991.[5]

In the cyber realm, the Stuxnet worm that induced a considerable number—perhaps as many as a thousand—of centrifuges in an Iranian nuclear facility to self-destruct in late 2009 and early 2010 provides another example of preventive force. It was clearly an act of prevention because its aim was to slow down a suspected nuclear weapons proliferation process. It was also considered an act of force because real physical damage—of the sort that commandos could have caused with bombs and bullets—was inflicted. But in this case the deed was done with bits and bytes.[6] The attack was not sabotage but rather what I call cybotage. This alternative to violence may have dissuaded the Israelis from mounting an Osirak-type operation—this time against the Iranians—and gained time for the diplomatic deal that followed.

The Osirak and Stuxnet examples highlight the point that in recent times, acts of preventive force have focused on counter-proliferation as a proximate goal. But clearly much serious thought has been given and continues to be directed to the idea that, in the future, preventive force, particularly in the form of cyber attacks like Stuxnet, may have the broader potential to take the place in statecraft of classic deterrence and coercive diplomacy.[7] The main point of attraction is that "cyber prevention" requires no major military field operations and may even be conducted covertly or deniably. Thus, both the costs and the risks of engaging in acts of preventive force may be sharply lowered. Taking preventive force into the virtual domain has the potential to revitalize this concept, which has significant historical roots, the analysis of which may provide immeasurable value in informing and guiding future actions.

The Classic Paradigm of Preventive Force

The archetypal historical instances that illuminate the application of preventive force are the two attacks conducted by the Royal Navy on the Danish fleet, the Danes' coastal artillery emplacements, and the city of Copenhagen in 1801 and 1807. On each occasion, in its continuing struggle against Napoleon, Britain feared that the Danes might employ their very considerable naval capabilities to close the Baltic Sea to trade in needed commercial goods and naval stores. Even worse was the dire possibility that formerly neutral fleets might actively join the French in a direct challenge to British naval mastery. In 1801 the threat to Britain took the form of an emerging League of Armed Neutrality, which comprised Denmark-Norway, Prussia, Russia, and Sweden. Rather, it was a "re-emerging

league," as the first such alliance was formed against British interference with neutral trade in 1780 during the American Revolution.

To parry the threat posed by the league, Britain dispatched a naval squadron to Denmark under the command of Adm. Sir Hyde Parker, a cautious man in his sixties who had recently enjoyed softer duty in the West Indies and married a teenaged girl. His second in command, Horatio Nelson—architect of earlier naval victories at Cape St. Vincent and the Nile—had a full understanding of the need to apply vigorous preventive force; indeed, he would defeat a larger force at Trafalgar some four years later. And in a hot action on April 2, 1801, at Copenhagen, the outcome was so much in doubt that Parker ordered Nelson to disengage. The latter famously chose to disregard Parker's command, and the Danes acquiesced. The British fleet went on to cow the other members of the league into submission.

According to the great naval historian Dudley Pope, "The destruction of a considerable part of the Danish Navy was eventually to benefit Britain before the war against France ended."[8] But the achievements of 1801 at Copenhagen were fated to be put to a fresh test. By 1807 the resentful Danes had rebuilt their fleet, and Napoleon had made himself master of much of Europe after decisively defeating Prussia and Austria and pummeling the Russians sufficiently to force them into an accommodation (and a kind of wary alliance via the Treaty of Tilsit).

The war aims on each side came to focus on imposing severe economic costs on the enemy. The French relied on their so-called Continental System, which was designed to limit any trade with Britain, while the latter's Orders in Council created a countervailing naval blockade in the hope that French commerce and credit would eventually be mortally wounded. At this point Britain had no immediate hope of defeating French land forces, so maintaining a favorable balance of naval power was crucial to its ability to continue the conflict. And it was British vulnerability at sea on which Napoleon fixed, in the belief that if he could but take control of the sizable, strong navy of Portugal and the revived Danish fleet and add them to his own and other captive warships, together they would make for a winning advantage. Indeed, as the apostle of sea power Alfred Thayer Mahan noted, Bonaparte "intended to seize the navies of Europe and combine them in a direct assault upon" Britain.[9]

However, not being favorably inclined toward the French, the Portuguese sailed their fleet away from Lisbon before Napoleon could grab hold of it. The situation with Denmark, whose navy had not only been reconstituted but improved in the wake of the 1801 incident, was far more dangerous. The Danes at this point were hardly on what could be called friendly terms with Britain. They also faced an implicit French threat of land invasion if Copenhagen reached any manner of accommodation with London. Thus, a new preventive naval expedition was decided on; it was to comprise more than fifty Royal Navy ships and twenty-five thousand army troops. The latter were to be at the ready to besiege the Danish capital as and if necessary.

Admiral Lord Gambier's fleet arrived off Copenhagen in August 1807. General Lord Cathcart's forces landed, under the direct command of Sir Arthur Wellesley, later the Duke of Wellington, and swiftly routed the Danish army. Still, the

fleet had to bombard Copenhagen for nearly four days early in September, causing terrible fires in the city, before the Danes agreed to hand over their ships. As Mahan summed up the results for the British, they "took possession of eighteen sail-of-the-line, besides a number of frigates, stripped the dockyards of their stores, and returned to England."[10] Napoleon's naval ambitions were thwarted.

For us today, the moral of these Napoleonic-era vignettes about the value of preventive force is that such short, sharp actions can have profound strategic impact. Bonaparte could never be truly secure, he knew, while Britain remained an implacable foe. But Britain could be countered only if its naval dominance were overturned. Only then could its support for the insurgency in Spain be cut off and its trade with Russia curtailed. As the historical record shows, Napoleon strove hard, over many years, to craft the kind of sea power that could achieve these aims and perhaps even to make the threat of invading Britain credible. The two preventive actions at Copenhagen kept sizable naval forces out of French hands, ensuring that British sea power would remain unbroken and—for the last decade of these wars—unchallenged.

Today, the strategic potential of preventive force remains as great, and the lower costs and risks of cyber prevention make this option even more attractive. Perhaps. But the very attractiveness of cyber prevention may prompt those who see themselves as potential targets to engage in policies and behaviors of an aggressive rather than an acquiescent nature. This was certainly the case in naval affairs, when aspiring sea powers operated under the constant fear that the Royal Navy might swoop in at any moment, as it had done twice against the Danes.

The Rise of a "Copenhagen Complex"

While the Danes were the direct victims of British preventive force and France had suffered the indirect strategic consequences, later in the nineteenth century Germany seemed most traumatized by a growing fear of a potential British coup de main mounted against its growing High Sea Fleet. In the wake of victorious land wars, culminating with the victory over France in 1871 that cemented German unification, Berlin began to focus seriously on naval affairs. This trend accelerated with the accession of Kaiser Wilhelm II, who was deeply taken with Mahan's ideas. After inviting Mahan to dinner on his yacht, the *Hohenzollern,* in 1893, the kaiser ordered that a German-language translation of Mahan's *The Influence of Sea Power upon History* be added to the onboard libraries of all German warships.[11]

The kaiser's determination to complement his land power with a first-rate navy led him into a key administrative alliance with the industrious Adm. Alfred von Tirpitz. In the decades before World War I, Tirpitz built a remarkably well-engineered fleet that was smaller than the Royal Navy but still quite substantial and in many ways superior, ship for ship. Regarding size, for example, in 1897 the German High Sea Fleet had less than a fifth the number of capital ships that the Royal Navy possessed, but by 1907 the Germans had closed the gap swiftly,

possessing nearly half as many all-big-gun battleships, or "dreadnoughts," as Britain's Grand Fleet.[12]

But the kaiser and Tirpitz, mindful of the British actions at Copenhagen, knew that as the fleet grew toward a point where it would have a deterrent effect on the Royal Navy—or failing that would be able to give a good account of itself in battle—the danger of provoking a preventive attack grew ever greater. And as Jonathan Steinberg once pointed out, as long as Britain "continued to expand its own fleet, the gap between the two powers, and thus the danger zone, would remain forever."[13] The omnipresent threat that the nascent Imperial German Navy might be "Copenhagened" helped to feed an antagonism toward Britain that accelerated shipbuilding. Thus, in 1912 when Winston Churchill called on the Germans to "declare a holiday" in the arms race, Kaiser Wilhelm seethed and refused even to respond.[14]

In the event, the Germans were not "Copenhagened"; indeed, the British did not use preventive force in the run-up to World War I. Further, the Battle of Jutland in 1916, in which a number of British battle cruisers blew up when hit, reflected a tactical victory for the less numerous German fleet. The British lost fourteen ships and more than six thousand sailors killed; the High Sea Fleet suffered eleven ships sunk and some two thousand men dead. Not enough damage was done to break the British blockade of Germany, but the High Sea Fleet had certainly shown itself to be a mortal threat to Britain—so much so that when serving as First Lord of the Admiralty, Winston Churchill held that the Grand Fleet commander was "the only man on either side who could lose the war in an afternoon."[15]

So here is an instance where fear of a preventive attack spurred a "proliferator" in an arms race to go fast, to take significant defensive steps—like mining sea approaches to home waters and widening an interior canal for secure big-ship movement—and to succeed in building up to a point where its capabilities posed a true and very dangerous challenge to British naval mastery.

What does the Copenhagen complex mean in the cyber era? Can one really draw an analogy between fleet bombardments and the use of cyber prevention? The answer is yes, if one accepts that cyber attacks will remain hard to detect and defend against. Certainly the aforementioned expert opinions surveyed in this chapter suggest that leak-proof defenses are unlikely to arise. Much as the Royal Navy could not be kept from sailing to Copenhagen, it will likely prove very difficult to seal out computer worms, viruses, Trojan horses, and the wide range of other malicious software. In the United States alone, the high-profile hacks of commercial and government sites suggest that cyber attack will remain a tool of choice for statesmen, insurgents, criminals, and others for many years to come.

Thus, in the wake of the Stuxnet attack, the Copenhagen complex remains relevant. Its principal implication is that the potential for the preventive use of "virtual force" could impel those who feel threatened to take significant steps both to mitigate the risk of being on the receiving end of such an action and to accelerate, expand, and more diligently secure their own efforts, especially in the

realm of developing weapons of mass destruction. For example, Iran, after the Stuxnet attack on its centrifuge program, quadrupled the number of centrifuges it deployed, bringing a burgeoning proliferation crisis with Tehran to a boil.[16] Was the alleged American-Israeli preventive use of force in this instance a boon or a bane? To be sure, the action gained some time for negotiation, but the proliferator's resolve to continue to possess an enrichment capacity was reaffirmed.

Whether the threat of another use of preventive force, either virtual or physical, will contribute usefully to sustaining the diplomatic solution now in place remains a vexing unknown at this point. This is particularly a risk for the use of advanced cyber techniques, which are to some extent "wasting assets." Once used, such exquisitely precise, targetable tools are unlikely to work as effectively when applied again. Patches will cover up specific vulnerabilities, and generally increased security awareness will stiffen defenses. These efforts will not eliminate the possibility of another use of cyber preventive force—new tools are always under development—but it does raise the cost of this form of intervention.

Another downside of the situation created by the Stuxnet exploit is that the very use of cybotage for preventive purposes, which may have gained time for diplomacy, opened a door to more general uses of cyber attack for retaliatory or signal-sending purposes. If the Shamoon virus that severely disrupted Saudi oil industry data was an Iranian attack, as many experts say, then it would be a logical follow-on to the Stuxnet operation's preventive use of cyber capabilities.[17] Thus, cyber as a mode of preventive force may seem more usable than violence, but it may also spawn more cyber wars. The matter is worth weighing in the balance as acts of cyber prevention are considered.

Other Lessons to Be Learned from the British: From Oran to Vemork

British leaders fully embraced preventive force in World War II. The most notable episode occurred after France fell in June 1940, when the Royal Navy's Force H sailed to the Algerian coast and bombarded the heavy French naval squadron in port at Mers-el-Kébir, near Oran. A brief, lopsided action saw one French warship sunk, others damaged, and over a thousand French sailors killed. Only one of the major combatant vessels escaped to Toulon, as did some of the lighter French ships in other parts of North Africa. Concurrent with the Oran strike (Operation Catapult), Operation Grasp undertook the seizure of other French ships and submarines that had made their way to British-controlled ports.

Britain took these steps to prevent the weak-kneed Vichy government from transferring the large French Navy to Germany. Winston Churchill, Britain's prime minister at the time, was deeply ambivalent but aware also of historical precedent and pressing need. In his history of the Second World War, he described the matter with sad eloquence: "This was a hateful decision, the most unnatural and painful in which I have ever been concerned. It recalled the episode of the destruction of the Danish Fleet at Copenhagen in 1801; but now the French had only yesterday been our dear allies, and our sympathy for the misery

of France was sincere. On the other hand, the life of the State and the salvation of our cause were at stake. It was Greek tragedy."[18]

No less a personage than Adm. Sir Andrew Cunningham, commander in chief of the Mediterranean Fleet, strongly opposed the preventive use of force, arguing that it would "alienate the French throughout the French Empire."[19] But action at Mers-el-Kébir did not lead to greater conflict, nor did a later attack at Dakar, where Vichy naval forces lost two submarines sunk and suffered serious damage to the battleship *Richelieu*. The French fought as hard as they were able against the British in these actions—much as the Danes had resisted so vigorously against Nelson in 1801—but as was the case with the Napoleonic-era preventive actions, these operations during World War II stayed contained too. To be sure, relations with the Vichy government were soured in part because of Oran and Dakar; this was a nontrivial cost of preventive action. But the gain—keeping the naval balance in Britain's favor—by far outweighed this political cost.

Beyond naval actions, the British used preventive force in other ways as well during World War II. Concerns arose about German progress toward building a nuclear weapons capability. While the Allies had the Manhattan Project under way, the Nazis also wanted to develop an atomic bomb. One of the principal components in the proliferation process was (and still is) heavy water, or deuterium oxide, which, very simply, slows down neutrons to the point where they can sustain a nuclear chain reaction using uranium-235 or other fissile material. In German-occupied Norway, the Norsk Hydro plant was able to produce heavy water and so became a serious concern of the Allies.[20]

Several attempts were made to destroy the plant. In the context of an ongoing conflict, repeated and protracted uses of preventive force may be needed and, thus, expected. Such was certainly the case when it came to slowing or stopping the German nuclear proliferation effort. First, British commandos tried an airborne assault, but it failed. Norwegian resistance fighters had their innings next and did some serious damage to production that took months to repair. Air raids followed. Hundreds of bombs were dropped on the plant, and the damage disrupted but did not cripple production. Nevertheless, all this attention prompted the Germans to try to relocate the heavy water stocks to relative safety closer to home. Thus, a big opportunity came when the Germans started to move the heavy water from Vemork in February 1944, with the first leg of the transit being by ferry across Lake Tinn. One Norwegian commando planted a bomb below the waterline of the vessel, and it detonated while the material was being ferried, sinking the boat and its cargo of heavy water. More than a dozen innocent Norwegian passengers died. Almost none of the heavy water was salvaged, dooming whatever small hopes the Germans had of bringing a nuclear reactor on line in time to build an atom bomb that might have changed their failing fortunes in the war.

The British use of preventive force during World War II reflected a clear willingness to move beyond single actions of relatively short duration and widely separated in time—like the strikes at Copenhagen in 1801 and 1807. To some

extent this was evident in the Royal Navy's actions against the French in 1940. As noted earlier, they were geographically quite widespread and waged over a period of nearly three months when one includes the action at Dakar. But looking beyond naval affairs to the counter-proliferation efforts against the heavy water facility at Vemork, one can glimpse the outline of an entire campaign of preventive force. This campaign took years; included several different forms of action, ranging from commando raids to aerial bombing; and concluded with the successful sabotaging of the Germans' attempt to move the heavy water to a safer location. The campaign was well worth the costs of the sustained effort. In the opinion of Kurt Diebner, one of the leading German atomic scientists of the wartime period, "When one considers that right up to the end of the war . . . there was virtually no increase in our heavy-water stocks in Germany, and that . . . there were in fact only two-and-a-half tons of heavy water available, it will be seen that it was the elimination of German heavy-water production in Norway that was the main factor in our failure to achieve a self-sustaining atomic reactor before the war ended."[21]

The key insight for the cyber era that can be drawn from British preventive practices during World War II thus may be to think about using cyber means of prevention in protracted campaigns—for example, against rogue proliferators, terrorists, and perhaps other adversaries—rather than restrict such actions to one-off events such as Stuxnet. Given that cyber measures can often be taken covertly—that is, with plausible deniability as to the identity of the perpetrator—and sometimes even clandestinely, with the target's being wholly unaware of the action taken, this notion of conducting protracted preventive campaigns grows more attractive. Indeed, the concept seems well suited to an era of perpetual irregular warfare. Whereas Winston Churchill found his choice to take preventive action against the French Navy in the summer of 1940 a "hateful decision," the decision maker today—and tomorrow—armed with cyber options may find fewer practical or ethical constraints standing in his or her way, whether the choice made is for a one-time coup de main or to pursue a more protracted preventive course.

While its potential for covert, deniable action may make protracted cyber preventive campaigns attractive, particularly in a time of open-ended conflicts with terrorists and proliferators, costs and risks are associated with such a longer-term approach. A strategic factor of concern is the likely loss of the veil of anonymity over time. When actions are aimed at clearly malevolent actors already being opposed openly, and perhaps even militarily, the costs and risks are acceptable. But a protracted cyber preventive campaign to counter a competing nation's aims in some theater of operations, or to curtail its continuing theft of intellectual property from one's own commercial sector, might come completely undone or lead to conflict escalation when the cyber exploits are "outed." A further though less critical risk is that in any protracted cyber prevention campaign, the tools being used will eventually lose their potency as the adversary's defenses improve. This problem can be mitigated by developing more tools, but it does impose a cost that needs to be considered.

Assessing the Prospects for Cyberspace-Based Preventive Force

Clearly much insight can be derived for our time, and the future, from the earlier history of preventive uses of force. Whether the intent is to stem the tide of proliferation or to preserve a favorable balance of power, the preventive use of force has proved a valuable tool of statecraft and strategy. Early in the cyber age, already one well-known example (Stuxnet) involves a computer worm inserted into a system to cause centrifuges employed in the nuclear enrichment process to self-destruct. One can only think that this covert, very low-risk means of intervention will continue to provide an attractive option to decision makers who are trying to cope with the potential threat of an adversary's "trading up" to nuclear-power status.

While preventing or delaying proliferation by means of cybotage highlights one aspect of maintaining a favorable balance of power, trying to shore up one's more traditional military edge over a competitor by cyber preventive means will likely be a daunting challenge. Certainly the pursuit of such an aim requires thinking in terms of more protracted preventive measures, which will involve coming back with cyber strikes again and again as needed—similar to the Royal Navy's return to Copenhagen in 1807, six years after the first preventive attack there. But the target set today, and on into the future, will be far more complex and will undoubtedly require taking aim at those civilian industries providing the advanced technologies on which their militaries depend. While a hard task, surely, it will be far from impossible. Indeed, the very porousness of cyber defenses of US high-technology firms has led to considerable hemorrhages of their intellectual property. And the same exploits that have led to such theft could just as easily be used to destroy or corrupt data in ways that slow or perhaps even reverse progress.

Whatever its ultimate limitations, cyber prevention's covert nature can still enable and empower protracted campaigns as opposed to limited, short-duration strikes against particular targets. If British strategists were committed to conducting attacks on French naval assets for months and then on the German nuclear program for years during World War II, there is little reason to believe that counter-proliferation via cyber means will be delimited from doing the same.

Of course, the demands of a more protracted approach to preventive action based on cyber capabilities will have some unique aspects of their own, with the principal one being that a method employed in one instance may not obtain over the longer term. This is because, once known, a cyber exploit may be straightforwardly defended against. Thus, a kind of wasting-asset feature to cyber methods must be considered, and any protracted campaign of prevention will have to be waged with an arsenal of unique exploits ready to be used one after the other. The value of a successful preventive action must be weighed against the cost of the future loss of use of any particular cyber weapon.[22]

Aside from defensive measures that might be taken by the adversary—as were so apparent in the Germans' attempts to protect their budding High Sea Fleet prior to World War I—the further problem is that a persistent fear of preventive

attack may spark very aggressive action, particularly in the form of arms racing. Again this can be seen in the case of Wilhelmine Germany, where the Copenhagen complex led to an accelerated pace of building all-big-gun battleships—considered the strategic weapon nonpareil of that time—in the hope that the "danger zone" might be escaped by the sheer speed of development and production.

Other forms of threatening action may be of a more covert nature—that is, designed to hide illicit or prohibited activity from view. One case in point of this latter type of (passive?) aggressive behavior is seen in the North Koreans' nuclear weapons program, which continued secretly in the wake of the 1994 Carter Accord and the much more fleshed-out Agreed Framework that, it seemed, had handled the problem.[23] It is now openly acknowledged that the United States considered the possibility of using preventive military force against North Korea and widely believed that Pyongyang had real fears of such an action being taken.[24] Yet, as in the case of the German High Sea Fleet, production efforts went ahead. In 2006 the North Koreans successfully tested a nuclear weapon and more recently have demonstrated their long-range ballistic missile capabilities. It is a cautionary tale for those who think the existential threat of preventive action alone might achieve the ends desired in any given interaction.

Cyber prevention mitigates this problem, at least to some degree. Striking with bits and bytes is, above all, a more usable option than attacking with bombs and bullets, especially in peacetime. Stuxnet's use may have been an act of war, but the identity of the perpetrator was never proved beyond a reasonable doubt.[25] Further, Iranian and international reactions were likely far more muted than would have been the case in the wake of an air raid, a missile strike, or a commando attack.

The next application of cyber preventive force may prove to be far less showy than Stuxnet, taking instead the form of deeply embedded malicious software that can, from time to time, conduct acts of cybotage or corrupt critical data in unseen, and unnoticed, ways. Both types of action—sporadic cybotage and manipulation of key data—might be used in protracted cyber prevention campaigns and could prove effective in the disruption of, say, an illicit weapons proliferation process. For more general purposes, these modes of cyber prevention could do a great deal to undermine the military effectiveness of potential adversaries, particularly those advanced enough to have developed dependencies on secure, ubiquitous flows of information in support of field operations. Indeed, it seems that although advanced information technology can do much to empower, at the same time it imperils. As Martin Libicki has observed, "The complexity of today's information systems is a central factor in making them vulnerable."[26] This makes for very fertile ground when it comes to taking a cyber approach to prevention.

Cyber prevention might also prove an ideal means for detecting and disrupting terrorist networks, for slowing their recruitment processes, and for generally undermining trust and morale. Dark networks are hard to deter or coerce, so preventive action may be the only way to keep their operatives from signing on, linking up, and then pursuing their murderous ways. Much as the British acted

to keep Napoleon from co-opting the navies of minor powers for conquest, so today cyber prevention may keep terrorist networks from rising to even more dangerous levels. Perhaps cyber prevention can even reverse their flow, sending terrorist networks down the path to ultimate defeat.

On balance, one can see considerable room for the application of cyber preventive force in the future, whether against rogue nations or terrorist networks. Will it lead to the kind of dystopian "cool war" world envisioned by the novelist Frederik Pohl, where a neo-Hobbesian war of all against all is waged but covertly?[27] Perhaps so. Perhaps such a development is unavoidable, as the merits of cyber prevention come to be more widely appreciated. Thus, the concept of preventive force may migrate from the physical to the virtual world and come back again.

Notes

1. "Danger," if to the point of an imminent threat of violent action, moves the issue from prevention to preemptive calculations about launching a "spoiling attack."

2. Thucydides, *The Peloponnesian War*, trans. Richard Crawley (New York: Modern Library, 1951), 50.

3. For a good survey of the ethical problems that attend preventive wars, see Deen K. Chatterjee, ed., *The Ethics of Preventive War* (Cambridge: Cambridge University Press, 2013). A more benign assessment of preventive war can be found in John Yoo, *Point of Attack: Preventive War, International Law, and Global Warfare* (Oxford: Oxford University Press, 2014). Yoo was a senior adviser to President George W. Bush on legal and ethical matters relating to the decision to invade Iraq in 2003, an act that supporters and detractors viewed as a quintessential case of preventive war.

4. Eisenhower's rejection of preventive war is discussed in John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of Postwar American National Security Policy* (Oxford: Oxford University Press, 1982), esp. 170.

5. The seminal study of this preventive action is Rodger W. Claire's *Raid on the Sun: Inside Israel's Secret Campaign that Denied Saddam the Bomb* (New York: Random House, 2004).

6. See Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014).

7. See, for example, Abraham Sofaer, *The Best Defense? Legitimacy and Preventive Force* (Stanford, CA: Hoover Institution Press, 2010).

8. Dudley Pope, *The Great Gamble: Nelson at Copenhagen* (New York: Simon & Schuster, 1972), 512.

9. Alfred Thayer Mahan, *The Influence of Sea Power upon the French Revolution and Empire*, vol. 2 (Boston: Little, Brown, 1898), 276.

10. Ibid., 277.

11. Barbara Tuchman, *The Proud Tower: A Portrait of the World before the War, 1890–1914* (New York: Macmillan, 1966), 152.

12. George Modelski and William Thompson, *Sea Power in Global Politics, 1494–1993* (Seattle: University of Washington Press, 1988), 76.

13. Jonathan Steinberg, "Germany and the Russo-Japanese War," *American Historical Review* 75 (1970): 1965–86. Steinberg also wrote on this theme in a key article, "The Copenhagen Complex," *Journal of Contemporary History* 1 (1966): 23–46; and in his other study of this era, *Yesterday's Deterrent: Tirpitz and the Birth of the German Battle Fleet* (Oxford: Oxford University Press, 1965).

14. See A. J. P. Taylor, *The Struggle for Mastery in Europe, 1848–1918* (Oxford: Oxford University Press, 1954), 501. Taylor goes on to note that Churchill repeated his call in 1913, and again the Germans refused to respond.

15. Geoffrey Bennett, *The Battle of Jutland* (London: B. T. Batsford, 1964), 155 and 42 for statistics on the battle losses and the Churchill quote, respectively.

16. See Ariane Tabatabai, "Hitting the Sweet Spot: How Many Iranian Centrifuges?," *Bulletin of the Atomic Scientists*, October 2014.

17. "U.S. Officials Believe Iran behind Recent Cyber Attacks," *CNN*, October 2012. See also Nicole Perlroth, "Cyberattack on Saudi Firm Disquiets U.S.," *New York Times*, October 24, 2012.

18. Winston S. Churchill, *The Second World War,* vol. 2, *Their Finest Hour* (Boston: Houghton Mifflin, 1949), 234.

19. Cited in Correlli Barnett, *Engage the Enemy More Closely: The Royal Navy in the Second World War* (New York: W. W. Norton, 1991), 175.

20. Even before the Germans invaded Norway, French intelligence had contrived a way to move Norsk Hydro's supply of heavy water (a little less than two hundred kilos) to France. But they left the plant untouched, so it remained a persistent threat.

21. Cited in Thomas M. Gallagher, *Assault in Norway* (New York: Harcourt Brace Jovanovich, 1975), 229. See also Dan Kurzman, *Blood and Water: Sabotaging Hitler's Bomb* (New York: Henry Holt, 1997), 238. He asserts that the preventive campaign "constituted the coup de grâce that finally doomed the German nuclear program."

22. Calculations of this sort are explored in a thoughtful study by Robert Axelrod and Rumen Iliev: "Timing of Cyber Conflict," *Proceedings of the National Academy of Sciences* 111, no. 4 (January 2014): 1298–303.

23. Former president Jimmy Carter, in his negotiations with the North Koreans, had gotten somewhat ahead of the Clinton administration in terms of commitments made, but the agreed framework ultimately followed his recommendations fairly closely. See International Atomic Energy Agency, "Agreed Framework of 21 October 1994 between the United States of America and the Democratic People's Republic of Korea" (Vienna: IAEA, November 2, 1994).

24. This is made clear in Joel S. Wit, Daniel B. Poneman, and Robert L. Gallucci, *Going Critical: The First North Korean Nuclear Crisis* (Washington, DC: Brookings, 2004).

25. However, reportage at the time suggested that Stuxnet was the product of an American and Israeli joint venture. See, for example, William Broad, John Markoff, and David Sanger, "Stuxnet Worm Used against Iran Was Tested in Israel," *New York Times*, January 15, 2011.

26. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007), 240.

27. See Frederik Pohl, *The Cool War* (New York: Ballantine, 1982).