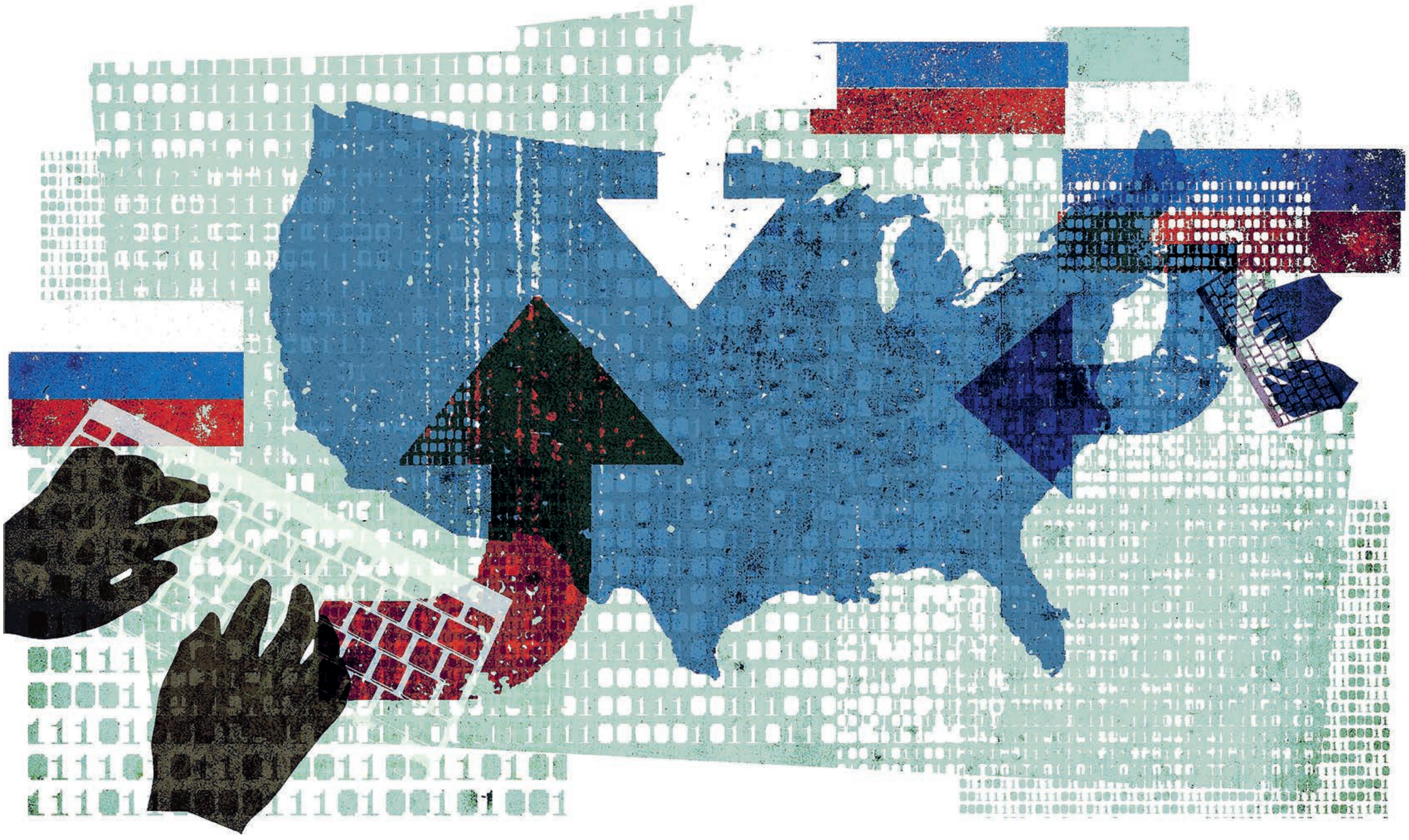
SECURITY BRIEFS

DETERRENCE IN THE CYBER AGE

Preventing a cyber-Pearl Harbor is not the only digital challenge nation states face



DPA/IKON IMAGES

BY JOSEPH S. NYE, JR.

Cyber security is a relatively new foreign policy problem. A decade ago it received little attention, but in 2013 the US Director of National Intelligence James Clapper declared cyber security risks to be the biggest threat facing the nation.

In 1996, only 36 million people or about 1 percent of the world population used the internet. In a mere two decades, that grew to half the world population. Now with big data, artificial intelligence and the "Internet of Things," the number of internet connections may grow to a trillion by 2030. The attack surface will expand, the number of actors will increase and attribution will be difficult. Can deterrence work in such a world?

Talk of a "cyber-Pearl Harbor" first appeared in the 1990s amid warnings about contaminated water supplies, disrupted financial systems and collapsed power grids. Despite many smaller attacks, such disasters have not yet occurred. Does that suggest that some kinds of deterrence work in the cyber age, or is it just too soon to know?

Deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit. Understanding deterrence in cyberspace is often difficult, because our minds are captive to Cold War images of deterrence as threatening massive retaliation to a nuclear attack by nuclear means. The analogy to nuclear deterrence is misleading, however, because the aim there is total prevention.

In contrast, many aspects of cyber behavior are more like other behaviors such as crime, which governments strive only imperfectly to deter. Moreover, cyber deterrence need not be limited to cyber responses. The political scientist Robert Jervis identified "three waves of deterrence theory" in the nuclear era. Theorizing about deterrence in the cyber era is emerging from only its first wave.

There are four major mechanisms to reduce and prevent adverse action in cyberspace: threat of punishment, denial by defense, entanglement and normative taboos. None of these four mechanisms is perfect, but together they illustrate the range of means by which it is possible to reduce the likelihood of adverse acts causing harm. They can complement one other by affecting actors' perceptions of the costs and benefits of particular actions. There is also an element of learning involved as states develop a more sophisticated understanding of the costs that are incurred in cyber warfare and as their economic dependence on the internet grows. Policy analysis focusing solely on punishment may miss some of the most important political behavior that indicates deterrence and dissuasion are working in the cyber realm despite the problem of attribution. In fact, while attribution is crucial for punishment, it is not important for deterrence by denial or entanglement.

Because deterrence rests on perceptions, its effectiveness depends on answers not just to the question "how" but also to the questions "who" and "what." A threat, defense, entanglement or norm that may deter some actors may not deter others. Similarly, it may succeed in regard to some actions but not others. Much depends on how actors perceive the capability and credibility of the deterrent instrument. As such, cyber deterrence resembles the concept of extended deterrence, in which a state attempts to protect an ally.

THE ANSWER TO WHETHER A POLICY OF DETERRENCE CAN WORK IN CYBERSPACE DEPENDS ON HOW, WHO AND WHAT

In the cyber realm, the effectiveness of deterrence depends on whom (state or non-state) one is trying to deter from which of their behaviors. Ironically, deterring major states from acts of force may be easier than deterring non-state actors from actions that do not rise to the level of force. The threat of a "bolt from the blue" by a major state has probably been exaggerated. Major state actors are more likely to be entangled in interdependent relationships than are many non-state actors. American declaratory policy has made clear that deterrence is not limited to cyber-against-cyber, although that is possible; deterrence can also be cross-domain or cross-sector with any weapons of its choice, including naming and shaming, economic sanctions and nuclear weapons.

The United States and other countries have asserted that the laws of armed conflict apply in cyberspace. For a cyber operation to be treated as an armed attack depends on its consequences rather than the instruments used. It is more difficult to deter attacks that do not reach the equivalence of an armed attack. Hybrid warfare, as in Ukraine, and information warfare exploit such gray zones. The 2016 Russian disruption of the US presidential campaign fell into such a gray area, and the Obama administration has been criticized for its inadequate response. For tactical reasons, the administration held back until too late, and the Trump administration failed to follow up. The result was inadequate deterrence and grave concerns for the future.

Yet even in gray zones, some progress has been made on deterrence. For years, the United States complained that China's cyber espionage for commercial advantage subverted fair trade and had enormous costs for the US economy. China, and other governments, lumped commercial espionage with general spying and rejected the development of a norm that would limit their exploitation of stolen intellectual property. The US indictment of five Chinese military officers for cyber theft plus the threat of further sanctions seems to have changed Chinese declaratory policy, and perhaps its behavior as well. On Sept. 25, 2015, President Barack Obama and President Xi Jinping agreed that neither government would "conduct or knowingly support cyber-enabled theft of intellectual property" for economic advantage.

The answer to whether a policy of deterrence can work in cyberspace depends on how, who and what. Ambiguities of attribution and the diversity of adversaries do not make deterrence and dissuasion impossible, but punishment occupies a smaller part of the policy space than in the case of nuclear weapons. Punishment is possible against both states and criminals, but attribution problems often slow and blunt its deterrent effects. Denial – through computer hygiene, defense and resilience – plays a larger role in dealing with non-state actors than with major states whose intelligence services can formulate an advanced persistent threat. With time and effort, a major military or intelligence agency is likely to penetrate most defenses, but the combination of threat of punishment plus effective defense can influence their calculations of costs and benefits, and thus far most attacks have involved gray zones rather than Pearl Harbors.

Policy analysts should not limit themselves to the classic instruments of nuclear deterrence – punishment and denial – as they assess the possibility of deterrence and dissuasion in cyberspace. They should also pay attention to the mechanisms of entanglement and norms. Entanglement can alter the cost-benefit calculation of a major state such as China, but it probably has little effect on a state such as North Korea, which is weakly linked to the international economic system. It affects non-state actors in different ways; some cyber criminals are like parasites that know they will suffer if they kill their host, but some dark-web criminals and terrorists may be indifferent to the damage they do.

Stability in cyberspace is difficult to predict, because the speed of technological innovation in the cyber realm is greater than in the nuclear realm. Over time, better attribution forensics may enhance the role of punishment; and better defenses through encryption or machine learning may increase the role of denial. The currently supposed advantage of offense over defense may change over time. Cyber learning is also important. As states and organizations come to better understand the limitations and uncertainties of cyber attacks and the growing importance of the internet to their economic wellbeing, cost-benefit calculations regarding the utility of cyber warfare may change just as nuclear learning altered analysts' understanding of the costs of nuclear warfare. Not all cyber attacks are of equal importance; not all can be deterred; and not all rise to the level of significant national security threats. The lesson for policymakers is to focus on the most important attacks as well as to understand the full range of mechanisms at their disposal and the contexts in which attacks can be prevented. One size does not fit all, and that is the key to understanding deterrence in the cyber age.

JOSEPH S. NYE, JR.
is a professor at the Harvard Kennedy School and author of the essay "Deterrence and Dissuasion in Cyberspace" in *International Security.*