Is There A Place For Nuclear Deterrence in Cyberspace?

By Timothy Farnsworth

In recent years, cyber attacks and the threats they pose have grown in sophistication, from low-level disruption and data theft—which are still a majority of cyber attacks—to high-level espionage and destruction.

Stuxnet, a piece of malware believed to be responsible for destroying approximately 1,000 centrifuges in Iran’s Natanz nuclear facility in late 2009 and early 2010, was a game-changer. For the first time, a computer virus was used to destroy a piece of physical infrastructure and the world took notice. The power of such a capability is clear today, but what happens once a wide range of countries and actors acquire equally sophisticated and powerful capabilities and there is no longer a technological gap between the United States, its allies, and the rest of the world?

While the prospect of a sophisticated cyber attack that could cripple critical infrastructure is currently unlikely, the potential is an ever-growing concern for government policy makers and military officials and has prompted a growing public debate about how to deal with the problem.

Should a country rely exclusively on its ability to defend and harden these critical networks against such attacks or should it also invest in new offensive cyber capabilities so that it can preempt or retaliate against such attacks? What can deter a state from launching major cyber attacks? Can states negotiate “rules of the road” for cyber behavior to help mitigate the threat?

Some policy makers and military leaders suggest that some cyber attacks fall under the nuclear deterrence umbrella. However, the threat of nuclear retaliation to a major cyber attack is neither proportional, nor credible, in stopping (deterring) high-level catastrophic cyber attacks against a nation’s critical infrastructure by other states, including the nuclear weapons complexes. As a result, nuclear deterrence cannot usefully be applied to the cyber realm and a more practical and effective approach to making cyberspace more secure and stable is needed.

U.S. Cyber Policy

Over the past four years, the United States has clarified its declaratory policy over how it views cyberspace and actions within it by state and non-state actors. In May 2009, President Obama said that cyberspace would be treated as a “strategic national interests” where the U.S. would “deter, prevent, detect, and defend against attacks.”

In May 2011, the White House released the International Strategy for Cyberspace. The document said, “When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country.” It went on to say, “[the United States] reserves the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with international law, in order to defend our Nation, our allies, our partners and our interests.”

In a November 2011 cyber report to Congress, the Defense Department said, “the President reserves the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interests from hostile
acts in cyberspace” and those “response options may include using cyber and/or kinetic capabilities provided by DoD” as long as such responses are proportional and follow international law of armed conflict.

According to the November 2011 report to Congress, “Deterrence in cyberspace, as with other domains, relies on two principle mechanisms: denying an adversary’s objectives and, if necessary, imposing costs on an adversary for aggression.” Achieving these objectives in cyberspace, however, has proven difficult for policy makers.

Nuclear Deterrence?

Some policy experts have reached back to the Cold War toolkit for ideas and are suggesting that there is a role for nuclear weapons to deter high-level, sophisticated cyber attacks by other nations against critical U.S. infrastructure. In February 2013, a Defense Science Board (DSB) task force released a report that recommended the United States continue to invest in its nuclear arsenal in order to deter highly sophisticated cyber attacks against its critical infrastructure and nuclear weapons systems by other nation states.

The study was commissioned by then-Undersecretary of Defense William Lynn to look at the resiliency of the Defense Department networks and weapons systems to cyber attacks. According to the report, the Pentagon has not kept up with “cyber adversary tactics and capabilities” and is “not prepared” to defend against a sophisticated cyber attack and would take years to build an “effective response” to the threat. It went on to say that the threat is “serious, with potential consequences similar in some ways to the nuclear threat of the Cold War.”

Foreign leaders are also comparing the threat of a serious cyber attack to one of a nuclear weapon. China’s Chief of the General Staff General Fang, after a recent meeting with the Chairman of the Joint Chiefs of Staff General Dempsey, said, “If control is lost over security in cyberspace, the effects can be, and I don’t exaggerate, at times no less than a nuclear bomb.”

The DSB said the only way to deter against such a devastating attack is to invest in cyber, conventional—including investing in Prompt Global Strike—and nuclear weapons. The report is careful to stress the need to invest in better cyber defenses and other, non-nuclear responses, so that a nuclear response is not the only option. However, the report states, “Nuclear weapons would remain the ultimate response and anchor the deterrence ladder.”

The DSB recommendation not only contradicts the decades long trend of reducing the role of nuclear weapons in deterring non-nuclear threats; it is inconsistent with the policies established by the 2010 Nuclear Posture Review (NPR) report. During the Cold War, both the United States and Russia held a broader definition of the role that nuclear weapons would play in deterring attacks. The two adversaries amassed nuclear weapons to deter and/or prevail in a nuclear exchange; to deter or respond to an overwhelming conventional attack; and to deter or respond to biological and chemical threats.

Over time, the role of U.S. nuclear weapons to deter strategic attack has been narrowed. The 2010 NPR, which lays out the current roles and missions of the U.S. nuclear weapons, came close to stating that nuclear weapons should only be used to deter a nuclear attack.

The NPR states that, “the fundamental role of U.S. nuclear weapons, which will continue as long as nuclear weapons exist, is to deter nuclear attack on the United States, our allies, and partners.” The NPR also says that role of nuclear weapons to deter “non-nuclear attacks—conventional, biological, or chemical—has declined
significantly.” The NPR stated that the “United States will continue to reduce the role of nuclear weapons in deterring non-nuclear attacks.”

The NPR makes no specific mention of the use of nuclear weapons to deter cyber attacks by other countries. The NPR states, for the first time, that it “will not use or threaten to use nuclear weapons against non-nuclear weapons states that are party to the Nuclear Non-Proliferation Treaty (NPT).”

DSB justified its recommendation by sighting part of the NPR that said, “[the United States] would only consider the use of nuclear weapons in extreme circumstances to defend the vital interests of the United States and its allies and partners;” a catastrophic cyber attack would meet this threshold the report said.

However, the threat of using nuclear weapons to respond to cyber attacks by other states against U.S. critical infrastructure is not a realistic nor an effective response to cyber attack because:

- Cyber attacks lack the destructive and existential threat of nuclear weapons;
- A nuclear response to a cyber attack is not proportional;
- Threatening to respond with a nuclear weapons lacks credibility in adversaries’ eyes;
- Cyber deterrence in general is difficult to achieve; and
- The policy would provide a new rationale for nuclear proliferators.

First, cyber attacks do not pose the same catastrophic threat nuclear weapons present. While it has been reported that the United States critical infrastructure is vulnerable to cyber intrusions and potential attacks, the likelihood of such attacks and their potential effects have been exaggerated by policy makers who lack the technical knowledge to predict accurately what effects a cyber attack might have on much of the critical networks.

With the exception of a cyber attack against a nuclear power plant that causes a nuclear meltdown—which is theoretically possible but very unlikely—there is no cyber attack with the destructive force of a “limited” nuclear attack involving less than 100 nuclear weapons, which could kill tens of millions of Americans immediately.

Even if an adversary were able to take down the power grid of the entire East Coast with a highly sophisticated cyber attack, leaving at-risk people populations and transportation systems vulnerable, such an attack would not have the nearly the same impact as the use of a few nuclear bombs on American cities.

This does not mean that there are not real vulnerabilities that need to be addressed before cyber weapons become even more capable and destructive. But for now, they are not. The United States should therefore focus on hardening these networks and working with the international community to establish rules of the road to decrease risk.

In March 2013 National Intelligence Director James Clapper presented the “Worldwide Threat Assessment” before Congress and said, there is a “remote chance” that over the next two years the United States will see a major cyber attack against its critical infrastructure, producing “long-term, wide-scale disruption of services, such as regional power outage.” However, it also said China and Russia “are unlikely to launch such a devastating attack” outside a “military conflict or crisis.”

Second, the law of armed conflict requires that states respond to aggressive acts of force proportionally. If cyber attacks lack the destructive force of nuclear weapons then responding to one with a nuclear weapon is not a proportional response. If China launched a cruise missile and took down a power plant, it would be disproportional to respond with launching a nuclear warhead at China. Now imagine that instead of a cruise
missile, a cyber attack is launched against the industrial control mechanism for the power plant and takes it offline. Does that somehow now warrant a nuclear response? No.

Third, U.S. adversaries are not likely to consider the threat of a nuclear response to a highly sophisticated or catastrophic cyber attack as credible. If, as a policy, nuclear weapons are included to deter any level of attack or behavior, it tends to lower its effectiveness. For the United States, a conventional military response is more appropriate and can more easily be calibrated to respond to highly sophisticated cyber attack and would therefore be seen as a more credible response by any potential adversary.

Fourth, a policy where nuclear weapons are used as deterrent against potential cyber attacks would have a negative effect on preventing nuclear proliferation. If responding to cyber attacks with nuclear weapons becomes an acceptable form of deterrence, it could legitimize other states’ nuclear weapons ambitions.

Fifth, deterring cyber attacks, whether low- or high-level, is generally difficult to achieve. The United States is more dependent on its information networks than many of its adversaries are, making it more difficult to threaten retaliation through cyberspace. In contrast to nuclear weapons, there are many more actors, state and non-state, that have cyber capabilities and less is known about these capabilities. And the technological bar for creating highly sophisticated cyber weapons is continuing to drop, allowing even more actors to have the capability of inflicting harm in the networks.

Finally, there is the attribution challenge. It could take months, years, if ever, for a country to definitively find who was responsible for a cyber attack. Now, many experts have stated that deterring cyber threats at the highest level of national security—state vs. state—is not as difficult because it still relies on traditional intelligence gathering and current geopolitical relationships and attitudes. However, traditional intelligence gathering and analysis makes mistakes and attribution often takes time, even against kinetic attacks.

A More Progressive Approach

United States is already investing and should continue to invest in defensive capabilities to build-up the resiliency of its critical infrastructure networks to cyber attack. If critical networks are more difficult to compromise, then adversaries will be less likely to target them. And, the further global integration of information networks makes it less likely that states will seek to disrupt or attack other states’ cyber networks because the economic effects would be too great for both countries.

The U.S. should also engage further the international community to establish acceptable “rules of the road” for state behavior in cyberspace. And, it is important that current international law be recognized as a guide for developing these cyber rules and adjusted in order to make sense in the new and different technological environment.

Several states, including the United States, have begun to discuss the establishment of cyberspace norms. The United Kingdom has hosted two international conferences on the subject. In September 2011 Russia and China proposed a code of conduct for cyber behavior. In 2011, the UN re-established the mandate for a group of governmental experts on developments in the field of telecommunications and international security. The United States and China recently discussed the possibility of opening a dialogue on the issue.

The adoption of a policy of using, or threatening to use, nuclear weapons in response to a major cyber attack by other states against U.S. critical infrastructure is not appropriate and is not an effective deterrent. Instead, the U.S. should continue to work with the international community to establish acceptable “rules of the road” that would hold states accountable and help impose some measure of restraint on all states’ cyber behavior.
Is There A Place For Nuclear Deterrence in Cyberspace?

One Response to Is There A Place For Nuclear Deterrence in Cyberspace?

Pingback: Nuclear weapons not an effective deterrent to cyber warfare « nuclear-news