ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Jason Healey

CYBER STATECRAFT INITIATIVE

Bringing a Gun to a Knife Fight: US Declaratory Policy and Striking Back in Cyber Conflict

If you pull a knife on a gunslinger, don't be surprised if you get shot. This is one of the messages of the president's International Strategy for Cyberspace. Some media outlets have taken to extreme headlines, such as OBAMA RESERVES RIGHT TO NUKE HACKERS, or HACK US AND WE'LL BOMB YOU. These headlines, although perhaps intended as hyperbole, highlight the routine misunderstandings that take place when applying national security concepts to the technical domain of cyberspace. This issue brief will analyze the relevant part of the Strategy, especially focusing on whether, and how, the United States might respond to cyber attacks, and under what circumstances, if any, such responses would be nuclear.

What the Strategy actually says is this:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners.
>
> We reserve the right to use all necessary means —diplomatic, informational, military, and economic — as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.

The Atlantic Council's Cyber Statecraft Initiative helps foster international cooperation and understanding of new forms of cooperation and conflict in cyberspace through global engagement and thought leadership. The initiative, in partnership with VeriSign, leverages the Atlantic Council's extensive global network of national security practitioners and experts to help create overlapping communities of interest with governments, non-government organizations and others working to solve challenges in cyberspace.

The Cyber Statecraft Initiative is generously supported by VeriSign.

This is an old-fashioned declaratory policy, a way to "suggest the circumstances under which the United States will consider specific retaliatory options" signaling "US perceptions of the gravity of specific acts," according to RAND. US national security strategists have been casting about for appropriate ways to deter devastating cyber attacks for years, and this is the strongest statement yet.

This statement is not directed at hackers, regardless of how annoying or how many .mil networks they may have intruded into. Declaratory statements like this are rather meant to deter high-end, destructive national security threats, generally (but not always) under the direction or coordination of other nations.

Cyber Declaratory Policy in Context

This part of the Strategy can be somewhat confusing, in that such declaratory statements have traditionally been associated with nuclear strategy, written for and by people

Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council of the United States. You can follow his comments on cyber issues on Twitter, @Jason_Healey.

more familiar with the writings of Schelling and Kahn than those of Spafford or Schneier. Hackers in particular seem to have misread it as a sign of their own importance.

To put the statement in context, here is summary of previous declaratory policies for nuclear arms from the Department of Defense's Nuclear Posture Review Report:

> During the Cold War, the United States reserved the right to use nuclear weapons in response to a massive conventional attack by the Soviet Union [and] to employ nuclear weapons to deter [chemical or biological weapon] attack on the United States and its allies and partners . . . The United States will continue to reduce the role of nuclear weapons in deterring non-nuclear attacks [and] will not use or threaten to use nuclear weapons against non-nuclear weapons states that are party to the [Nuclear Non-Proliferation Treaty].

The declaratory policy (and indeed, the whole International Strategy for Cyberspace) should be seen as an extension of America's broader national security policy, which has long preserved the option of asymmetrical—yet proportional—response as a means of deterrence.

In particular, compare the declaratory statements on cyber to those in the President's 2010 National Security Strategy:

> Military force, at times, may be necessary to defend our country and allies or to preserve broader peace and security. . . We will draw on diplomacy, development, and international norms and institutions to help resolve disagreements, prevent conflict, and maintain peace, mitigating where possible the need for the use of force.
>
> While the use of force is sometimes necessary, we will exhaust other options before war whenever we can, and carefully weigh the costs and risks of action against the costs and risks of inaction. When force is necessary, we will continue to do so in a way that reflects our values and strengthens our legitimacy, and we will seek broad international support, working with such institutions as NATO and the UN Security Council.
>
> The United States must reserve the right to act unilaterally if necessary to defend our nation and our interests, yet we will also seek to adhere to standards that govern the use of force.

Both White House documents cover parallel points, including self-defense; unilateral action as an option, but collective response as a preference; and the appropriate use of all aspects of national power, with military force as a last resort, and all responses rooted in national values. Interestingly, one of the more accurate assessments of this part of the strategy came from the *China Daily*, which wrote that "the White House made it clear that the US will use its military might to strike back if the country comes under a cyber attack that threatens national security." The *Voice of Russia* had a similar assessment, albeit phrased in more judgmental terms: "Washington, as always, enjoys the right to eliminate the threat with commensurate force, including launching surgical strikes on any country."

So in one sense, the declaratory policy in the International Cyber Strategy is a relatively boring affirmation of continuity, that the statements in the National Security Strategy apply to cyberspace, the modality of an attack is not important, only the fact of it. But of course, there is more to this than just a restatement.

Cyber theorists have long thought that nations may try to hide behind a veil of Internet anonymity in order to launch with impunity damaging cyber attacks on the United States, the national security version of "Nobody knows you're a dog." Richard Kugler expressed it this way: "Cyber attacks are often regarded as not deterrable because they are 'free rides'—the attacker has an expectation of impunity—but this calculus could be changed by creating expectations that cyber aggression might be an uncertain or costly act."

The administration's new declaratory policy is a direct attempt to so change an adversary's calculus. If a nation's leadership launches an attack against the US that nation must understand the consequences if they are caught, or even strongly suspected. Plausible deniability (whether through Internet anonymity, routing an attack through another country, or enlisting non-state proxies) may seem to be poor judgment. And even if an adversary only brings a knife to the showdown, they have been warned that the US won't feel constrained to leave the six-guns in their holsters.

This ups the stakes for cyber attacks, making it clearer to any attackers that if the US or its allies suffer a significant attack, they can expect appropriate retaliation in any form

that suits—a statement fully in compliance with international law. If the United States, or any other nation, were attacked on the seas, the President would not be limited to retaliating solely by using the US Navy. An attacked nation is free, bounded by proportionality and related legal norms, to choose from a variety of responses, whether it be in land, air, sea, cyberspace.

Restated this way, the declaratory policy seems less provocative; indeed, it isn't even the first time this has been said by a president. President Bush's 2003 National Strategy to Secure Cyberspace laid out a similar declaratory policy:

> When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the US response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner.

The new policy improves on its predecessor, being both clearer and more prominent (the 2003 statement was buried on page 50 of 54). But, more importantly, the new statement does not just threaten a response—it puts conditions on that response. Too many commentators have highlighted the eyeball-grabbing threat of US TO BOMB HACKERS without mentioning the less-inflammatory provisos, including "We will exhaust all options before military force," and "seeking broad international support."

Responding to Cyber Conflict

The headlines also imply that the US would resort to "nukes" over mere annoyances—that at some point, when too many web pages have been defaced, the White House will unleash SEAL Team 6. This has not been, and will never be, the case. While the topic of retaliation to cyber attacks can be a convoluted topic (veteran cyber conflict researcher Martin Libicki at RAND has dedicated an entire chapter to it in his 2009 book, *Cyberdeterrence and Cyberwar*) some things are clear.

Most importantly, there are existing norms and government process in place—imperfect, but well understood and long-standing—to ensure that the US only brings its guns to a gun- or a knife fight, not just a schoolyard shoving match. Any decision to respond with kinetic military power will not be made lightly, and will be rooted in existing international law, such as the "armed attack" threshold from the United Nations Charter. In short, if a cyber attack hasn't killed anyone or caused significant property damage or a deep and prolonged hit to GDP—the normal indicators of war—do not expect any kinetic response, much less a fission-based one. Choices to respond to major cyber attacks will be made by the President, supported by the Principals Committee of the NSC, likely after reviewing options developed in an interagency policy committee and already chewed over by a Deputies Committee. The Principals on the NSC are senior decision-makers who are used to making difficult choices with deadly consequences, and based on less-than-perfect information. If the President and his NSC can decide to strike across international boundaries on a fifty-fifty chance to kill bin Laden, then they likely can handle the ambiguities of cyber response more ably than many commentators anticipate.

Also often overlooked are the available nonmilitary tools, of diplomatic, informational, and economic options – such as sanctions, public statements from senior officials, or revoking of visas. The National Security Council would likely reach first for these options to respond to many kinds of cyber conflict, such as a repeat of the 2007 attacks against Estonia. Indeed, the US seems to be laying the groundwork for possible intervention in future Estonia-like situations when it says in the Strategy that cyber conflicts "could compel actions under the commitments we have with our military treaty partners," such as NATO, where an attack on one is an attack on all.

Going Nuclear?

Articles that highlight the "nuclear" aspect of cyber conflict are indulging in hyperbole, as there has apparently not even been a single death resulting from a cyber attack. Few cyber conflicts will even rise to the level of war, much less nuclear war, yet the nuclear comparison persists. For example, according to RAND's Libicki, "[F]or a while, it was Russia's declared policy to react to a strategic cyber attack with the choice of any strategic weapon in its arsenal."

The US has never explicitly threatened to use nuclear weapons over cyber attacks, as Russia has, but it is also standard practice for the US to never take military options off the table. For example, a 2009 article quotes General Kevin Chilton, then-commander of US Strategic Command, and thus responsible for both nuclear and cyber forces, as insisting that all options, including nuclear, should be available to respond to cyber attacks. But for the US (or any

nation) to consider responding with nuclear weapons—for the first time in more than sixty years—a cyber attack would have to be equivalent in effect to a massive, even thermonuclear explosion: thousands dead and massive damage. There are few realistic ways a cyber attack could inflict such a catastrophe, and even if such an event did occur, most nuclear powers have many other kinetic military options short of going nuclear.

What Else?

This declaratory policy is a major step forward in improving transparency into US decision-making for cyber conflict; however, more could be said. The Strategy did not, for example, specifically place any limits on "first-use cyber attacks against civilian infrastructure" or "damaging networks of financial institutions," as recommended by Richard Clarke and Robert Knake in 2010.

Although not mentioned in the Strategy, the United States military appears to already have some such limitations at the operational level. For example, General Keith Alexander, the commander of US Cyber Command, testified before Congress that the "law of war principles of military necessity, proportionality, and distinction will apply" to cyber operations. This implies that some kinds of targets may not be struck—that the US military will not directly target hospitals or civilians not involved in an adversary's war effort. Also, it means the US would forego some kinds of cyber military capabilities, such as those that cannot be adequately controlled after release and would therefore be more likely to cascade uncontrollably and disproportionately.

More specifically, General Alexander testified that it "is difficult for me to conceive of an instance where it would be appropriate to attack a bank or a financial institution, unless perhaps it was being used solely to support enemy military operations." This view is likely driven by both legal considerations (such as not being proportional, because of the overall negative effect on civilians) and domestic pressure (since the US will suffer more than other nations if finance is considered a legitimate target).

This leads to two findings: First, observers outside the American national security apparatus should understand that the declaratory position is more complex than what is implied by the single paragraph in the Strategy. According to Greg Rattray, former NSC staffer and author of the groundbreaking 2001 *Strategic Warfare in Cyberspace*, this is typical: declaratory policies are always a collection of diverse policies, speeches and actions. Second, those inside the American national security apparatus should understand that even statements of the obvious—such as foregoing attacks against hospitals or other obviously prohibited targets—may still be appreciated by the international community, since so much in cyber conflict is still uncertain.

Importance of a Cyber Declaratory Statement

National security policymakers in the United States have been concerned about the lack of a clearly stated cyber declaratory policy for years. So, one advantage of this new policy is that it shifts the debate from the *need* to the more-productive concern regarding whether this is the *right statement to make*, and, if not, how to improve it. More importantly, the declaratory policy puts conditions on an American response that should improve transparency and give pause to would-be cyber attackers.

Despite the attention it has gotten, the declaratory policy, while important, needs to be taken within the context of the larger Strategy. Though they did not make for such splashy headlines, other parts of the Strategy—such as the clear statement of applicable norms, commitment to Internet freedom, and the backing of multi-stakeholder Internet governance—will likely be more important over time than the declaratory statement.

Some technologists are disappointed that this Strategy has little to say about making the United States less vulnerable to knife wounds, but these statements are meant for other nations' militaries and decision-makers—not their (or US) technologists. Those leaders will likely understand this message and the consequences of lightly provoking a knife fight with the United States. Those adversaries may still consider relying on Internet anonymity to hide their attacks, but, all of a sudden, that "veil" may seem quite a bit thinner in the face of a possible US kinetic military response. The result here, as in so many areas of cyber conflict, remains to be seen.

SEPTEMBER 2011

The Atlantic Council's Board of Directors

CHAIRMAN
*Chuck Hagel

CHAIRMAN, INTERNATIONAL ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

CHAIRMAN EMERITUS
*Henry E. Catto

VICE CHAIRS
*Richard Edelman
*Brian C. McK. Henderson
*Richard L. Lawson
*Virginia A. Mulberger
*W. DeVier Pierson

TREASURERS
*Ronald M. Freeman
*John D. Macomber

SECRETARY
*Walter B. Slocombe

DIRECTORS
*Robert J. Abernethy
Odeh Aburdene
Timothy D. Adams
Carol C. Adelman
Herbert M. Allison, Jr.
Michael A. Almond
*Michael Ansari
Richard L. Armitage
Adrienne Arsht
*David D. Aufhauser
Ziad Baba
Ralph Bahna
Donald K. Bandler
Lisa B. Barry
*Thomas L. Blair
Susan M. Blaustein
Julia Chang Bloch
Dan W. Burns
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Daniel W. Christman
Wesley K. Clark
John Craddock
Tom Craren
*Ralph D. Crosby, Jr.
Thomas M. Culligan
Gregory R. Dahlberg
Brian D. Dailey
*Paula Dobriansky
Markus Dohle
Lacey Neuhaus Dorn
Conrado Dornier
Patrick J. Durkin
Eric S. Edelman
Thomas J. Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Dan-Åke Enstedt
Julie Finley
Lawrence P. Fisher, II
Barbara Hackman Franklin
*Chas W. Freeman
Jacques S. Gansler
*Robert Gelbard
Richard L. Gelfond
*Edmund P. Giambastiani, Jr.
*Sherri W. Goodman
John A. Gordon
*C. Boyden Gray
*Stephen J. Hadley
Mikael Hagström
Ian Hague
Harry Harding
Rita E. Hauser
Annette Heuser
Marten H.A. van Heuven
*Mary L. Howell
Benjamin Huberman
Linda Hudson
*Robert E. Hunter
Robert L. Hutchings
Wolfgang Ischinger
Robert Jeffrey
*A. Elizabeth Jones
*James L. Jones, Jr.
George A. Joulwan
Stephen R. Kappes
Francis J. Kelly
L. Kevin Kelly
Zalmay Khalilzad
Robert M. Kimmitt
James V. Kimsey
*Roger Kirk
Henry A. Kissinger
Franklin D. Kramer
Philip Lader
Muslim Lakhani
David Levy
Henrik Liljegren
*Jan M. Lodal
George Lund
Izzat Majeed
Wendy W. Makins
William E. Mayer
Barry R. McCaffrey
Eric D.K. Melby
Rich Merski
Franklin C. Miller
*Judith A. Miller
Alexander V. Mirtchev
Obie Moore
*George E. Moose
Georgette Mosbacher
Bruce Mosler
Sean O'Keefe
Hilda Ochoa-Brillembourg
Philip A. Odeen
Ahmet Oren
Ana Palacio
Torkel L. Patterson
*Thomas R. Pickering
*Andrew Prozes
Arnold L. Punaro
Kirk A. Radke
Joseph W. Ralston
Norman W. Ray
Teresa M. Ressel
Joseph E. Robert, Jr.
Jeffrey A. Rosen
Charles O. Rossotti
Stanley Roth
Michael L. Ryan
Marjorie M. Scardino
William O. Schmieder
John P. Schmitz
Jill A. Schuker
Kiron K. Skinner
Anne-Marie Slaughter
Alan Spence
John M. Spratt, Jr.
Richard J.A. Steele
Philip Stephenson
*Paula Stern
John Studzinski
William H. Taft, IV
John S. Tanner
Peter J. Tanous
Paul Twomey
Henry G. Ulrich, III
Enzo Viscusi
Charles F. Wald
Jay Walker
Michael Walsh
Mark R. Warner
J. Robinson West
John C. Whitehead
David A. Wilson
Maciej Witucki
R. James Woolsey
Dov S. Zakheim
Anthony C. Zinni

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Harold Brown
Frank C. Carlucci, III
William J. Perry
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
James R. Schlesinger
George P. Shultz
John Warner
William H. Webster

LIFETIME DIRECTORS
Lucy Wilson Benson
Daniel J. Callahan, III
Kenneth W. Dam
Stanley Ebner
Carlton W. Fulford, Jr.
Geraldine S. Kunstadter
James P. McCarthy
Jack N. Merritt
Steven Muller
Stanley R. Resor
William Y. Smith
Helmut Sonnenfeldt
Ronald P. Verdicchio
Carl E. Vuono
Togo D. West, Jr.

** Members of the Executive Committee*
List as September 15, 2011

The Atlantic Council of the United States is a non-partisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.