ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Jason Healey

CYBER STATECRAFT INITIATIVE

Preparing for Cyber 9/12

Experts have warned about a massive surprise cyber attack since at least 1991, when Winn Schwartau testified to Congress about the dangers of an "electronic Pearl Harbor." More recently, the analogy has changed to a "cyber 9/11" but the fear is generally the same: the dependence of modern economies and societies on cyberspace means a digital attack could fundamentally disrupt our way of life and be remembered for decades as the day everything changed.

Unfortunately, the analogy is rarely ever taken any deeper to uncover new truths and infer others. Instead "cyber 9/11" is used as shorthand to scare people into noticing the dire consequences of dependence on a cyberspace combined with gaping vulnerabilities and in the face of a menacing online threat. Clearly, more wisdom is needed.

To help add depth to the idea of a cyber 9/11, this Issue Brief examines what might happen the day *after* a major cyber disruption, on 9/12. Starting with important lessons – based on the findings from a major conference – the Brief concludes with three key recommendations: First, the cyber and national security communities on both sides of the Atlantic must continue to regularly convene for scenario-based events. Second, decision makers should trust their national security instincts when facing cyber crises. Third, we must finally break the fifteen-year public-sector/private sector stalemate.

Lessons Learned

A combination of exercise and conference, the Cyber 9/12 event shed light on several broad lessons:

International cyber crisis management is critical but there may be less than expected disconnect between US and European approaches. As summarized by a European former official, "a cybercrisis may take an international dimension at once, with events happening in many countries simultaneously." The required international collaboration is not practiced nearly enough. As another senior European participant put it, "Development of international cyber crisis management approaches is probably the most significant challenge we have in defending and deterring against global cyber threats."

There is not much reason to imagine that defenders or policy makers from the United States or Europe would have common views about how to respond to a cyber catastrophe. Yet surprisingly, there were no major disconnects between participants from nearly 20 countries at the Cyber 9/12 event. Representatives from the US government used similar language and had similar thresholds for actions and response plans as did those from European governments and NATO. Likewise, large telecommunications carriers had the same concerns and expectations whether they were from Europe or the United States.

The private sector is critical to an effective response after an event, but remains disconnected from government. The private sector is responsible for the vast majority of power lines, server farms, financial networks, and other major systems that would likely be targeted by an

About the Cyber Statecraft Initiative

The Atlantic Council's Cyber Statecraft Initiative helps foster international cooperation and understanding of new forms of competition and conflict in cyberspace through global engagement and thought leadership.

The first event of the "Cyber 9/12 Project" – to determine how the transatlantic community would respond after a cyber catastrophe – was held on December 8, 2011, in Washington, DC.

This project was made possible by the generous support of SAIC.

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

adversary planning to cause a cyber 9/11 event. However, there remains a major disconnect between the public and private sectors.

The Cyber 9/12 participants highlighted a "clash of cultures" because the telecommunication sector is "multi-stakeholder, open, and flat; by contrast, government is hierarchical and secretive." For example, individuals in the biggest global telecommunications providers come together in very tight-knit groups with high levels of mutual trust in order to defeat large attacks and keep the network resilient. The government lacks this agility, but has more capability and endurance to work difficult problems over long periods of time.

Worse, because of the relative power of the private sector in cyberspace, there will be a tug-of-war over with governments. As one European government participant expressed it,

> Try to imagine NATO running the Kosovo bombing campaign through the NAC while at the same time engaged in 27 different dialogues with bits of the Confickr Working Group and various companies within the global telecommunications industry. Add to that the fact that each of those three groups would think that they ought to be in charge, and then throw in the media, and you start to get a sense of the challenge.

This difference in cultures has made cooperation and trust more difficult since the participants agreed that, "It does not make any difference whether you are in government or not; people will only work with those they already have a trusting relationship with."

Though the problem is very marked in the United States, it is not universal. Jean-Francois Pacault, formerly with the French Ministry of Finance and Industry, noted this trust does exist there, with the result that "the technology sector, though not so developed as the United States, works more closely with the government."

The media plays an important role to connect the government, private sector and the public – but it is a role confusing to all. The media has a particularly novel role in cyber conflict. Though the government regularly classifies (and overclassifies) national security information, rarely does that information so directly involve individual citizens or private sector companies who are being directly targeted by hackers and spies. Since the information coming from the government is lacking, this puts the media in the lead for putting relevant national security information in the hands of defenders, something not found in other national security conflicts. Also, cyberspace is a highly technical topic, meaning the media coverage is often in the more technical trade press, or in the "Technology" section rather than "World." And of course, cyber conflict – indeed, all things "cyber" – are new and unfamiliar to the press just as much as it is for the government and most of the public.

In a crisis such as the one in the Cyber 9/12 scenario, these trends would be particularly troublesome. Just when many private security researchers would be clamoring to release results for press coverage, the government would likely be especially tight lipped, since a foreign nation is clearly involved.

In some scenarios, attribution for cyber attacks, long considered unsolvable, may in fact be quite easy. "Attribution" for a cyberattack is shorthand for the process of trying to determine who launched it. This is usually a long and

Cyber 9/12 Conference Event

In partnership with SAIC, the Atlantic Council convened the "Cyber 9/12 Project: Cyber Statecraft after Catastrophes" to determine how the transatlantic community would react the day after a major calamity in cyberspace.

Panelists representing industry, academia, and US and other governments grappled with the questions raised by the scenario. The group stopped frequently to hear feedback from designated observers and discuss issues with the audience from nearly twenty different nations in Europe, Asia, and North America.

The scenario, challenging and plausible, saw Iran deliberately challenging the West with non-lethal cyber attacks. Since their purpose was to shore up public support internally and in the international community, the Iranian government did not hide their involvement. By the end of the scenario, the Iranian government had severed submarine cables disrupting 80% of transatlantic communications.

As the scenario developed, the audience was often asked to judge, using a ten-point scale, how responsible Iran was for the attack. This scale and the results will be discussed later in this paper.

highly technical process and many cases end up as simply unsolvable. Fortunately, the information the policy makers most need can often be had without having to rely on solving these difficult forensic challenges. As one participant with a long history in cyber conflict observed, "It might not be a certainty that Russia was behind the 2008 cyber attacks on Georgia, but as it was indeed the Red Army tanking across the Georgian border around the same time, I'm willing to make the leap. The more significant a cyber event, the more likely there will be a geopolitical context that provides at least signposts to attribution."

In the conference scenario, Tehran made it clear that it was conducting and encouraging these attacks to coerce the West and would continue until appeased. Using a draft version of the Spectrum of State Responsibility (see Table 1), which has been recently published by the Atlantic Council[1], the consensus of the audience was that the first round of attacks were probably not directly conducted by the Iranian regime, but instead were somewhere in the wide gap between "state-encouraged" and "state ordered." That is, the Iranian government knew about the attacks and was, at a minimum, egging the attackers on. The ultimate authorship of the attacks was not in any doubt.

Even without iron-clad attribution – and the possibility of being wrong – having "good-enough" attribution enables other levers of national power, and most of them don't involve coercion. There are also many non-technical means to determine if the nation was behind the attack. Most importantly, does the suspected adversary cooperate when asked? The Russian government was the only government to refuse to provide the Estonians any information on the 2007 attack, even though they'd signed an official sharing agreement. Even if doing so was out of pure stubbornness or national pride, the government of a nation that refuses to cooperate after a cyber attack that impinges on national security cannot blame anyone but themselves if their intransigence bolsters suspicions of complicity.

Nations will respond to national security cyber emergencies by adapting their existing mechanisms for real-world geopolitical crises. Once the crisis in the Cyber 9/12 event escalated to where it was clearly an Iranian government attack, participants, from both sides of the Atlantic, treated this not as a cyber crisis, but a geo-political crisis that happened to impact cyberspace.

"The more significant a cyber event, the more likely there will be a geopolitical context that provides at least signposts to attribution."

Table 1:
The Spectrum of State Responsibility

1. **State-prohibited.** The national government will help stop the third-party attack
2. **State-prohibited-but-inadequate.** The national government is cooperative but unable to stop the third-party attack
3. **State-ignored.** The national government knows about the third-party attacks but is unwilling to take any official action
4. **State-encouraged.** Third parties control and conduct the attack, but the national government encourages them as a matter of policy
5. **State-shaped.** Third parties control and conduct the attack, but the state provides some support
6. **State-coordinated.** The national government coordinates third-party attackers such as by "suggesting" operational details
7. **State-ordered.** The national government directs third-party proxies to conduct the attack on its behalf
8. **State-rogue-conducted.** Out-of-control elements of cyber forces of the national government conduct the attack
9. **State-executed.** The national government conducts the attack using cyber forces under their direct control
10. **State-integrated.** The national government attacks using integrated third-party proxies and government cyber forces

1 Jason Healey, "Beyond Attribution: Seeking National Responsibility in Cyberspace", Atlantic Council, 2012.

The US may be seen as a natural leader by international partners. While there is "no maestro for this orchestra" the United States will remain the indispensible power to resolve crises in cyberspace. One European former official explained it this way, "Owing to its superior technical competence and strategic position with managing the Internet, the US is the natural leader for the technical part of the crisis; beyond that technical stage is the realm of international politics, which is another story and has its own customs."

National security cyber crises will have both technical and political responses. Attacks that may not be particularly interesting from a technical perspective may nevertheless have critical implications for international security. For example, the early attacks in the Cyber 9/12 event were not seen as a catastrophe by network defenders. But what made these attacks far more worrying was that a nation state was first encouraging them and then taking full responsibility. This political dimension grafted an additional level of response: how would nations respond to the national challenge from Iran that happened to be expressed in cyberspace?

Had this been a real event, rather than a fictional scenario, national ministries of defense and foreign affairs would be holding special meetings with allies and like-minded nations to find solutions. At those meeting, the Iran desk heads would have the lead, rather than cyber experts. In the United States, the situation would rapidly escalate up to the National Security Council which would coordinate the response.

So, once the incident crosses the threshold to be politically interesting, nations and international organizations would exercise their normal crisis management procedures. None of the responses discussed above would be significantly different if Iran had chosen to behave badly by threatening terrorist attacks, closing the Straits of Hormuz, rather than a cyber attack. This political dimension makes the technical community somewhat uncomfortable.

Thresholds for response and NATO's Article 5. If a cyber conflict is serious enough to draw in political leaders there will of course be discussion (or at least speculation) of kinetic response and collective defense, which for NATO members would mean a decision by the North Atlantic Council to invoke Article 5 commitments. These dynamics are similar regardless of whether the disruption was caused by cyber or kinetic attacks. The scope, duration and intensity of cyber attack would likely need to be similarly destructive as a large kinetic attack (hundreds or thousands dead, significant destruction) and conducted by an external actor to clearly rise to the Article 5 threshold.[2]

> *"The government of a nation that refuses to cooperate after a cyber attack that impinges on national security cannot blame anyone but themselves if their intransigence confirms suspicions of complicity."*

For example, the consensus during the Cyber 9/12 event was that nations would be very unlikely to respond with kinetic attacks until Iran itself crossed that same threshold and took kinetic action that cause significant casualties. Most participants felt their national governments might start to consider kinetic attacks in response only when the fictional Iranian attacks severed submarine cables (disrupting 80 percent of transatlantic traffic). But even here, governments would be unlikely to escalate to military attacks since the Iranian attack did not cause any direct casualties, meaning Article 5 would not have come into play.

Recommendations

The first event of the Cyber 9/12 Project successfully combined the private experience of an exercise with the public knowledge of a conference. Based on the discussions and interactions, there are clear recommendations for policy makers.

The cyber and national security communities on both sides of the Atlantic must continue to regularly come together for scenario-based events. The world has faced only a small set of the kinds of conflicts that are possible in cyberspace. Scenario-based events are perhaps the best way to phrase better questions and find better answers.

Conferences on cyber conflict all too often conclude discussions of tough topics with "we must further study these questions" or conclude that "it depends." The advantage of

2 For more on cyber and Article 5 see Jason Healey and Leendert Van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today and Tomorrow", Atlantic Council, 2012.

scenario-based events, like the Cyber 9/12 Project, is that they channel discussions to more concrete consensus, in this case: "Even if Iran followed this course, it would not be an armed attack under the UN Charter and we would not be anywhere close to Article 5. The United States would not strike back kinetically."

Decision makers should trust their national security instincts when facing cyber crises. The Cyber 9/12 event clearly showed that while cyber catastrophes will have their own character they are not especially different from other kinds of geopolitical crises. Nations will largely use norms and thresholds rooted in traditional national security fundamentals. National response, at the political level, will use tried-and-true crisis management frameworks. Whether in cyberspace or in the land, sea, air or space domains, nations are most likely to attack during times of spiking geopolitical tensions. And attribution, while perhaps not often reliable to determine if nations are responsible for criminal or espionage acts in cyberspace, can be incredibly simple for the most disruptive attacks. It is difficult for one nation to coerce another just by using covert attacks of any kind. To get a message across clearly, sometimes a national leader will just speak plainly.

Of course, national security decision makers should get advice from cyber conflict experts, but can rely on their existing base of knowledge, experience and instincts.

Break the fifteen-year public-sector/private sector stalemate. The need for information sharing and trust between the government and private sectors has been well known since before 1998, when US President Clinton issued a decision directive calling for cooperation. Yet nearly fifteen years later, the same findings surface in every exercise and report and are met with the same platitudes and saccharine commitments and action plans. It should be clear that "more of the same" will not be enough, though specific proposals are out of the scope of this paper.

The world will likely, at some point, be faced with a calamitous attack in cyberspace. Causing death, destruction and global disruption, a cyber 9/11 will immediately spark a change in the world – everything the day after such an attack will be different than the day before. The findings and recommendations from the first Cyber 9/12 event will hopefully be an important step in preparing for that fateful day.

MAY 2012

The Atlantic Council's Board of Directors

CHAIRMAN
*Chuck Hagel

CHAIRMAN, INTERNATIONAL ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

VICE CHAIRS
*Robert J. Abernethy
*Richard Edelman
*C. Boyden Gray
*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
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
Lisa B. Barry
*Thomas L. Blair
Julia Chang Bloch
Dan W. Burns
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
Daniel W. Christman
Wesley K. Clark
John Craddock
David W. Craig
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
*Stephen J. Hadley
Mikael Hagström
Ian Hague
Rita E. Hauser
Annette Heuser
Marten H.A. van Heuven
*Mary L. Howell
Benjamin Huberman
*Robert E. Hunter
Robert L. Hutchings
Wolfgang Ischinger
Robert Jeffrey
*James L. Jones, Jr.
George A. Joulwan
Stephen R. Kappes
Francis J. Kelly
L. Kevin Kelly
Zalmay Khalilzad
Robert M. Kimmitt
Roger Kirk
Henry A. Kissinger
Franklin D. Kramer
Philip Lader
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
Teresa M. Ressel
Jeffrey A. Rosen
Charles O. Rossotti
Stanley Roth
Michael L. Ryan
Harry Sachinis
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
James B. Steinberg
Philip Stephenson
*Paula Stern
John Studzinski
William H. Taft, IV
John S. Tanner
Peter J. Tanous
*Ellen O. Tauscher
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
William Y. Smith
Helmut Sonnenfeldt
Ronald P. Verdicchio
Carl E. Vuono
Togo D. West, Jr.

**Members of the Executive Committee*
List as of April 24, 2012

The Atlantic Council is a nonpartisan 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.

1101 15th Street, NW, Washington, DC 20005 (202) 463-7226
www.acus.org