ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Jason Healey

CYBER STATECRAFT INITIATIVE

When "Not My Problem" Isn't Enough: Political Neutrality and National Responsibility in Cyber Conflict

Since the Internet makes us all neighbors, more nations are likely to be affected by conflicts in cyberspace than in the air, land, or sea. Nations are increasingly looking to limit potential cyber conflicts using the same devices that have limited more traditional wars: treaties, conventions, and norms.

One of the most important global norms has been a state's rights to remain neutral in response to international conflict, as guaranteed by the Hague Convention. But because of the nature of engagement and conflict in cyberspace, it is still unknown how well the old agreements will hold up, and what must be reinvented.

As Internet protocols themselves route cyber attacks through any number of neutral countries, cyber conflicts are usually not so destructive as to obviously trigger international law. This may also render the identity or nationality of belligerents uncertain.

Legal norms based on the Hague Convention will likely be less useful than were a modified norm of *political neutrality* where nations should come under political pressure to take reasonable steps to stop cyber attacks, regardless of whether the responsibility is codified in a formal treaty. The problem of defining political neutrality in cyber conflict may well give rise to new norms of international engagement. If so, the "not my problem" excuse will no longer be acceptable.

Cyber Conflict and Neutrality: How Did We Get Here?

The obvious starting point in this discussion is the meaning of *neutrality*. Though the concept is an old one, the current legal international concept was codified in the Hague Convention of 1907, which states clearly, "The territory of neutral Powers is inviolable." The US Department of Defense defines neutrality in international law as an "attitude of impartiality" that sets rights and duties between impartial and belligerent states.

There are no definitive documents which address neutrality in cyber conflict, nor the obvious ways in which cyber neutrality differs from the more established domains of land, air, sea, and space. While the US government has been very clear that it will treat cyberspace as it does these other domains, neutrality has gotten very little attention and much of this is focused on only one area, the implications of a cyber attack routed from or originated through a third country. However, this ignores many other important topics. What, for example, were the neutrality implications of the decision by a US internet service provider to host the Georgian president's

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.

This is an edited version of a paper that first appeared in the Proceedings of the 4th International Conference on Cyber Conflict, held by the NATO CCDCOE in Tallinn, Estonia in 2012.

This paper was made possible by generous support by The Morganti Group Inc.

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**.

"Nations should come under political pressure to take reasonable steps to stop cyber attacks, regardless of whether that responsibility is codified in a formal treaty."

website following the Russian invasion of Georgia in 2008? As Stephen Korns and Joshua Kastenburg have discussed, this was presumptively a legitimate target during an international armed conflict that was now located on US soil.[1] As they note, "the unregulated actions of third-party actors have the potential of unintentionally impacting US cyber policy, including cyber neutrality. There is little, if any, modern legal precedent."

Political (Rather Than Legal Neutrality) in Cyber Conflict

Even in the traditional domains it may not always be clear how to apply the Hague guarantee that "The territory of neutral Powers is inviolable." But cyberspace compounds those problems geometrically.

The Internet protocols themselves route cyber attacks through any number of neutral countries in ways that may not be known–or even predictable–by a belligerent. Moreover, the cyber conflicts seen so far are typically criminal intrusions, denial of service attacks, nuisance attacks by bored or aggressive hackers, or espionage. None of these obviously rise to the level of "armed conflict" or other thresholds required for most international laws on conflict to apply. Even in conflicts with clear national security implications (such as Estonia in 2007 and Georgia 2008) the disruption caused was short-term, reversible, and did not appear to have caused any human casualties. Lastly, the identity or nationality of the belligerents may not be obvious. Indeed, the target of an attack may not even know they are under attack.

All of this makes a strict legal approach, bound to existing treaties, problematic. Even more problematic would be attempting to modify existing treaties, as the world has only seen a subset of the likely kinds of conflict in cyberspace. Modifying treaties to accommodate only those cyber conflicts we have seen so far would be myopic; modifying them to include those we have not yet seen, and can only imagine, would be folly.

Political neutrality fills this gap, especially as it can operate under the strict legal thresholds and be always applicable. In contrast to the more strictly defined legal norms of the Geneva and Hague Conventions, political neutrality allows a wider range of expectations and responses. Since it is judged by heads of state and public opinion, rather than international tribunals, it establishes in essence a separate set of norms for international behavior.

How Can a Nation Be Less Than Neutral in a Cyber Conflict?

Most legal literature on neutrality and cyber conflict focuses on a single issue posed by the ICRC: "Does routing of attacks by a belligerent state through the internet nodes of a neutral country violate its neutrality?" This is perhaps the wrong perspective, given the kinds of cyber conflict to date, as embodied in the 2007 attacks on Estonia.

A better phrasing may be "During a conflict, what obligations does a State have to stop attacks coming from its territory or citizens?" This similar, but broader, question encompasses the possibilities that a State will still have responsibilities not only when a belligerent routes traffic through its "internet nodes."

During the Estonia crisis, most attacks were not "routed" in the way we normally think of a weapon system being routed. These attacks were not predominantly cyber "missiles," launched from the government of one belligerent and passing through the territory of other nations on their way to the target. Rather, most of the 178 nations would have either (1) hosted infected computers (called bots or zombies) that were under the control of non-state actors in one belligerent

"Modifying treaties to accommodate only those cyber conflicts we have seen so far would be myopic; modifying them to include those we have not yet seen, and can only imagine, would be folly."

1 Stephen W. Korns And Joshua E. Kastenberg, "Georgia's Cyber Left Hook," Parameters, Winter 2008-2009.

country, or (2) been the location from which non-state patriot hackers launched such attacks in support of their original motherland.

Indeed, being the source of attack traffic is the most visible way that nations can lose their political neutrality in a cyber conflict. Here is a more inclusive, but still partial, list:

1. Hosting bots in its physical territory.
2. Hosting command and control nodes of a network of bots (i.e., a botnet).
3. Attacks pass through physical territory on their way to the target.
4. Residents in its physical territory are participating in the attack.
5. Hosting legitimate military or dual-use targets of interest to one of the belligerents.
6. Hosting chat rooms that are coordinating the attack.
7. Senior leaders are encouraging attacks.
8. Refusing to respond to requests for help.

For a State to consider itself strongly neutral, it should be working to mitigate all of these symptoms of partiality – many of which fall under other obligations, such as the Council of Europe´s Convention on Cybercrime of 2001 (Budapest Convention).

This flips the legal norm on its head. Because attacks are internationally routed in ways that may not be knowable to an attacker, the traditional norm placing responsibility on the attacking belligerent becomes highly problematic, at times nonsensical. Some of this responsibility must be picked up by nations along that attack path to take reasonable steps to mitigate the attack, if they can.

In Context: An Example of Cyber Conflict

To help pull apart these threads of political neutrality, the following example gives a realistic conflict scenario.

Phase 1: Zendia directs its hacker groups to deface and disrupt webpages of the Muragian leadership, and the Muragian networks of banks, utilities, and online stores. The botnets used in the attack come predominantly from five countries: Zendia, Trissalia, Floria, Pollabia, and Glospland. The attacks cause no casualties or significant disruption,

"For a State to consider itself strongly neutral, it should be working to mitigate all symptoms of partiality."

though they are inconvenient. In response, Muragia asks for assistance. Zendia and its client Trissalia unsurprisingly refuse to take any action since they are behind the attack to begin with. While Floria attempts to stop the attacks but cannot, lacking technical and law enforcement capacity, Pollabia and Glospland are both able to stop the attacks from their own territory. Muragian hackers launch their own counterattack, but the Muragian government clamp down on the activity very quickly.

In addition to formally making *demarches* to the unhelpful countries, Muragia protests formally in regional security forums and at the United Nations Security Council and General Assembly.

Phase 2: Muragia's defenses have become significantly better at blocking attack traffic, so Zendia sends teams to both Trissalia and Floria to build additional attack infrastructure and enlist other hackers. Now, these countries are not just the source of botnet traffic, they have Zendian hackers conducting attacks from their own soil. In addition, Zendia has initiated a new line of attack. Rather than launching massive (and noticeable) denial of service attacks from botnets, they begin "low and slow" intrusions, routed through all the countries involved. These are hard to detect, even by watchful defenders using advanced gear.

Muragia feels that Trissalia and Floria, with attack teams on their own soil, have far stronger responsibilities now that their role in the crisis is more direct. Unfortunately, the Florian government is still unable to stop the attacks, and Trissalia unwilling. Muragia also asks countries to stop the "low and slow" attacks, but as these are so difficult, it does not complain when little help is forthcoming.

Phase 3: The attacks ratchet up as nearly 200 people have been left dead and injured after the disruption of traffic lights, hospital networks, and local electrical power. Floria, which had been unable to stop the attacks earlier, realizes the change in the nature of the conflict and implements a heavy handed, but effective stop to the attacks from their territory. The heads of state of Floria, Pollabia, and Glospland come together to demand first that Zendia cease to use their

territory in the onslaught against Muragia, and threaten a response. Some of their more academic-minded international lawyers resist, saying there is far from a clear cut case that the Zendian leadership is truly responsible. Even if they were, the law is far from clear unless the UN Security Council acts. Glospland goes further, saying the attacks must stop, from wherever their source, or else there will be a military response. In the meantime, they implement sanctions, use their diplomats and political leaders to vilify Zendia, and use other levers of power.

Understanding Political Neutrality in Cyber Conflicts

As noted earlier and illustrated by this example, there are many ways a nation can be less than neutral in a cyber conflict. Accordingly, this means there are many shades of responsibility each nation can bear but, as yet, there has not been any easy way to categorize these. To understand this example, the Spectrum of State Responsibility[2] (see Table 1) is helpful – but not conclusive – to determine how neutral a nation really is. This spectrum assigns ten categories, each marked by a different degree of responsibility, based on whether a nation ignores, abets, or conducts an attack.

How politically neutral are each of the five countries in the earlier example? **Zendia** proved itself as not at all neutral. Indeed, it should be considered a belligerent, as it actually "ordered" the attacks (rather than merely ignoring, encouraging, shaping, or coordinating them), putting it at level 7 in the spectrum. **Muragia** was also a belligerent, because it was the original party under attack. However, it brought its own hackers under control. **Trissalia** did not order any attacks, but clearly provided all support to one side, the Zendians, and ignored requests from the other party. This means it is at least at level 3 of ignoring the attacks. **Floria** and **Pollabia** responded neutrally, though the former's response was feckless, putting these countries at levels 2 and 1 respectively. **Glospland** acted neutrally in stopping the attacks, putting it at level 1, but did later support Muragia as the party facing the online aggression.

As the scenario proceeded, though the spectrum remained helpful, there were obviously other factors in play. The most important of these are the overlapping criteria of severity, obviousness, "stoppability," and duration.[3]

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.

- **Severity:** Some conflicts are more dangerous than others; the more intense and deadly, the stronger the requirement for positive actions to remain neutral.
- **Obviousness:** Some attack patterns are far more evident which implies a stronger responsibility for a nation to not allow them if they want to remain neutral.

2 For more details, see previous cite for Healey, "Beyond Attribution: Seeking National Responsibility in Cyberspace", *supra* note 12.

3 Note these are related to, but not identical to the "scope, duration and intensity" test for whether an attack reaches the threshold of "armed attack" in the UN Charter (see Thomas Wingfield and others).

- **Stoppability:** Some attack patterns are far easier to restrict which implies a stronger responsibility for a nation to not allow them.
- **Duration:** The longer the cyber conflict, the stronger the need for a country to take actions to remain neutral. A single attack packet that passes through the nation's system deserves less response than a campaign lasting months.

These important points often seem undervalued or even ignored in the current discussion. The norms of politically neutrality seem hard to find and weak. Yet they are not only realistic but help to give far more clarity on the appropriate norms. Once there is a more severe crisis with casualties and real damage, political neutrality will become more important. In the same way, discussion on political neutrality must distinguish between those attacks which are most easily detected and stopped, as there is a higher obligation to stop these.

Commercial Neutrality

The dominant difference between conflict in cyberspace and that in other domains is not the speed of operations, nor the fuzziness of borders, nor its global reach. While important, these are dwarfed by the fact cyberspace is owned and operated overwhelmingly by the private sector. Any conflict with national-security relevance will be fought in the networks and systems of individual companies which built them for their own purposes, and which may decide they want nothing to do with the conflicts of their host nations.

For example, imagine if there were a repeat of the 2007 attacks against Estonia. Microsoft, McAfee, Symantec, Kaspersky and other companies may want to be seen as neutral, providing impartial service to both belligerents. They may not be able to, however, either because of a government's order or because one side sees them as being a tool of, or disproportionately helping, the other.

Indeed, commercial pressures already enforce something very much like commercial neutrality. Bill Woodcock describes the long track record of successful cooperation between the world's largest network providers to stop the most disruptive attacks. He describes a common scenario where one provider, say in the United States, may see a massive attack coming from their connection from an Internet exchange point in, for example, London. These major providers have a special authenticated hotline system, for the

"Any conflict with national-security relevance will be fought in the networks and systems of individual companies which built them for their own purposes, and which may decide they want nothing to do with the conflicts of their host nations.

Could there even be a major cyber conflict if the global network providers decided to suppress it?"

US downstream provider to contact the upstream provider in London, to ask them to stop the attack streams, since they are just being dropped by the US provider. This is usually in everyone's interest, since the upstream provider is paying to send this traffic which will never be delivered, taking up their bandwidth in the meantime. Why pay to send bits that will never be delivered? Indeed, it is then in the downstream provider's interest to ask for a cessation of attack traffic from whatever provider is sending into them, who can continue this chain to the originating network owner.

This process is not being done for any reasons related to 'neutrality,' and certainly not because of any articles of the Hague Convention. They do it because it is cheaper, more efficient, and just good behavior — a very commercial, but no less beneficial, norm. This kind of action is well outside the reach of what most Western governments could achieve, yet it is being done routinely without their need to be involved.

In the future, commercial neutrality will become ever more important as power is likely to continue to shift away from central governments and to non-state actors (like companies). Indeed, could there even be a major cyber conflict if the global network providers decided to suppress it?

Policy Recommendations

Political neutrality will be an important norm for future cyber conflicts, and states will soon be unable to sit back and say "not my problem" as attacks transit their networks. The following recommendations should aid states in adopting policies better suited to addressing future cyber conflict.

1. **Clean our own cyberspace.** The United States must take responsibility for monitoring and reducing malicious traffic on its own networks.
2. **Incorporate contingency plans into incident responses.** We must ensure that our incidence response plans involve contingencies to manage requests for help by other countries experiencing cyber attacks. With diplomatic pressure, we must also encourage other countries to do the same.
3. **Engage the private sector** in efforts to stop transnational cyber attacks, as its role in cyber conflicts is dominant in the cyber domain.
4. **Incorporate the norm of political neutrality** into international negotiations regarding cyber engagements and conflicts, before the conflicts themselves arise.

SEPTEMBER 2012

Visit **www.acus.org** for other publications from the Cyber Statecraft Initiative:

- Preparing for Cyber 9/12
- The US Cyber Policy Reboot
- The Spectrum of National Responsibility for Cyberattacks
- The Five Futures of Cyber Conflict and Cooperation
- NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow
- Beyond Attribution: A Vocabulary for National Responsibility for Cyberattacks
- Bringing a Gun to a Knife Fight: US Declaratory Policy and Striking Back in Cyber Conflict

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
Michele Flournoy
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
Robert M. Gates
Michael G. Mullen
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 July 1, 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