2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

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

Jason Healey
Cyber Statecraft Initiative
Atlantic Council
Washington, D.C., U.S.A.
jhealey@acus.org

Abstract: Cyber conflict may not be new, but it is far from old. And as with any other major, disruptive global trend, there are vexing questions on which traditional international norms still apply, whether they apply but with modifications, or whether entirely new norms must be invented. One of the most important norms has been for states to be able to remain neutral in response to international conflict, with rights and responsibilities guaranteed by the Hague Convention. Because of the nature of cyber conflict, such legal norm may be less useful than a modified norm of *political* neutrality. The Internet protocols themselves route cyber attacks through any number of neutral countries, cyber conflicts are usually not so destructive to obviously trigger international law, and the identity or nationality of the belligerents may not be obvious.

Nations might (and probably *should*) accordingly come under political pressure to take reasonable steps to stop cyber attacks, regardless of whether or not it is a formal treaty obligation. This paper explores this issue and ways a nation may be less than neutral, tying this to a ten-point spectrum of state responsibility to help determine just how responsible a nation might be in a cyber conflict. To illustrate potential new norms in action, the paper then describes a notional cyber conflict which shows how the nations' rights and responsibilities are influenced by the four factors of severity, obviousness, "stoppability," and duration. The paper concludes with a short section on the commercial neutrality during cyber-conflict, given the critical role that the private sector has played in the creation and operation of cyberspace.

Keywords: *neutrality, cyber conflict, national responsibility, Hague Convention, Law of Armed Conflict, political neutrality, commercial neutrality*

1. INTRODUCTION

Since cyberspace makes us all neighbors, more nations are likely to be affected by conflicts in cyberspace than in the air, land or sea. These nations will have to take more active steps to stop attack traffic if they wish to remain neutral.

Nations are increasingly looking to limit future conflicts, to bring these under more control, just as more traditional wars were restrained through treaties, conventions and norms. But it is still unknown how well the old agreements will hold up and what must be reinvented because of the nature of cyberspace and cyber conflict.

One of the most important norms has been for states to be able to remain neutral in response to international conflict, with rights and responsibilities guaranteed by the Hague Convention. Because of the nature of cyber conflict, such legal norm may be less useful than a modified norm of *political* neutrality. The Internet protocols themselves route cyber attacks through any number of neutral countries, cyber conflicts are usually not so destructive to obviously trigger international law, and the identity or nationality of belligerents may not be obvious.

Nations might (and probably *should*) accordingly come under political pressure to take reasonable steps to stop cyber attacks, regardless of whether or not it is a formal treaty obligation. This paper examines one aspect of this, political neutrality in cyber conflict. New norms will develop as "not my problem" will no longer be acceptable.

This paper will start the examination of political neutrality with a literature review of neutrality and cyber conflict, especially the legal aspects which features in most of the literature. However, after this introductory section, the paper shifts from legal to political neutrality, which allows more flexibility to adapt to the nature of cyber conflict. After this, the paper moves on to specific ways a nation could be less than neutral, tied to a ten-point spectrum to help understand responsibility and neutrality. A notional example of a cyber conflict illustrates how political neutrality might work in practice and highlights four factors likely to influence political neutrality – severity, obviousness, "stoppability," and duration – and areas for further research.

2. CYBER CONFLICT AND NEUTRALITY: HOW DID WE GET HERE?

The obvious starting point in this discussion is "what is meant by neutrality?" Though the concept is an old one, the current legal international concept was codified in the Hague Convention of 1907, which discusses rights and duties, and begins as clearly as possible, "The territory of neutral Powers is inviolable." A definition that seems to be widely used is one from the dictionary published by the U.S. Department of Defense (DoD). Neutrality here is defined as in international law, the attitude of impartiality during periods of war adopted by third states toward a belligerent and subsequently recognized by the belligerent, which creates rights and duties between the impartial states and the belligerent.[1]

1 JP 1-02, "DoD Dictionary of Military and Associated Terms", January 2012, p. 234.

This definition lacks mention of neutrality in cyber conflict, but this is no surprise as it does not discuss the obvious ways neutrality differs in the other domains of land, air, sea or space either. The U.S. government has been very clear that it will treat cyberspace as it does these other domains, not least for the applicability of international law.

The White House International Strategy for Cyberspace declared that "Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace."[2] Similarly, the commander of Cyber Command in testimony to Congress declared, "all military operations must be in compliance with the laws of armed conflict—this includes cyber operations as well. The law of war principles of military necessity, proportionality and distinction will apply [...]"[3] If needed, one provision of the 1934 Communications Act allows the President to close down communications stations and remove equipment if needed, to "in order to preserve the neutrality of the United States."[4]

Most of this recent attention, however, has been focused only on two areas: how the United States would respond to an attack on itself (or its allies) and how the laws of armed conflict (LOAC, also known as International Humanitarian Law or IHL) apply to offensive military operations. There has been little or no mention of how neutrality applies to cyber other than an implication it would be handled similar to any other domain. This is not straightforward, of course.

The only official U.S. document that goes into any depth on neutrality in cyber conflict is a 1999 document from the DoD General Counsel, *An Assessment of International Legal Issues in Information Operations*.[5] This early paper covered an impressive range of issues relating to cyber operations (though they were not then called by that term) including neutrality and "self-defense in neutral territory." This paper made several important contributions, including making it clear that

- "If a neutral nation permits its information systems to be used by the military forces of one of the belligerents, the other belligerent generally has a right to demand that it stop doing so."
- "A neutral Power is not called upon to forbid or restrict [communications], so long as such facilities are provided impartially to both belligerents."
- The use of a "nation's communications networks as a conduit for an electronic attack would not be a violation of its sovereignty in the same way that would be a flight through its airspace by a military aircraft."
- Nations need not have much concern "for the reaction of nations through whose territory or communications systems a destructive message may be routed."
- "Transited state would have somewhat more right to complain if the attacking state obtained unauthorized entry into its computer systems as part of the communications path to the target computer."

2 White House, International Strategy for Cyberspace, 2011, p. 14.
3 General Keith Alexander, Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command, 2010, p. 15.
4 Communications Act of 1934, Section 606c.
5 Department of Defense General Counsel, *An Assessment of International Legal Issues in Information Operations, May 1999.*

The general US approach, to treat cyberspace as similar to other domains, is supported by material from the International Committee of the Red Cross, whose work is based on the Geneva and Hague Conventions that are a foundation for LOAC. An official paper from 2004 by Knut Dörmann, Deputy Head of the ICRC Legal Division, argues that under the Geneva Convention (and its Additional Protocols, signed but not ratified by the United States), "the fact that a particular military activity constituting a method of warfare is not specifically regulated, does not mean that it can be used without restrictions."[6] This paper discusses many ways that LOAC would apply to cyber operations, but includes little on neutrality. Andrew Carswell, an armed forces delegate to the ICRC, has gone farther to describe their view on neutrality in a 2011 presentation. Starting with an explanation of the Hague Convention laws (and a sense they have a "slightly musty quality") he examines several scenarios on how neutrality might apply to cyber conflict.[7]

Neutrality in cyber conflict is vexed by any number of challenging questions, such as these, from a paper by Sean Kanuck, now a senior U.S. intelligence official:

1. "What if a neutral party did not know when its sovereignty was breached to conduct an attack or was technically incapable of restricting belligerents' use of its […] networks without irreparably harming its own governmental functions or economy?
2. "What if the tools required to conduct or defend against a cyber attack needed to be pre-positioned in global networks to be most efficacious?
3. "What if a sovereign did not exercise due diligence in preventing its own subjects from criminally compromising foreign computer systems and later using them to attack a third sovereign nation?"[8]

To help the discussion move past theoretical questions, two military officers from a U.S. military cyber defense unit took the discussion in a very practical direction. Stephen Korns and Joshua Kastenburg examined one of the most important international cyber conflicts, the Russian invasion of Georgia in 2008, when a U.S. internet service provider hosted the website of the Georgian president, with important implications for America's role as a neutral or belligerent. Korns and Kastenburg, as one of the few full-length treatments on the subject provide an excellent definition of legal cyber neutrality:

> "Cyber neutrality, therefore, is the right of any nation to maintain relations with all parties engaged in a cyber conflict. Under a traditional international law rubric, to remain neutral in a cyber conflict a nation cannot originate a cyber attack, and it also has to take action to prevent a cyber attack from transiting its Internet nodes."[9]

6 Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks," 2004, p. 2, *available at* http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

7 Andrew Carswell, "Neutrality in Cyberwar," Presentation To The Internet In Bello: Seminar On Cyber War, Ethics & Policy, UC Berkeley School of Law, 2011, *available at* http://www.law.berkeley.edu/files/Neutrality_in_Cyber_War_for_web.pdf.

8 Sean Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law," Texas Law Review, Vol.88, Issue 7, 2010, p. 1593.

9 Stephen W. Korns And Joshua E. Kastenberg, "Georgia's Cyber Left Hook," Parameters, Winter 2008-2009, p. 62.

Korns and Kastenburg also highlight an important additional aspect that is rarely mentioned in other works, the role of the private sector, which dominates in cyberspace in a way they do not in other domains, with important implications for neutrality. According to their paper,

> "Private industry owns and operates the majority of the Internet system. During a cyber conflict, 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."[10]

Kastenburg later wrote a follow-up article in a U.S. Air Force Law Review that also examined this incident but with a more legal perspective.[11]

This focus on real-world events marks an important trend in the literature, an increasing focus not on the *legal* implications of neutrality, but the *political* importance. After all, nations can still insist other nations take actions to mitigate the effects of a cyber conflict, even if international lawyers are still parsing over "musty" treaties and arguing over the meanings.

This expectation that nations have some positive obligation to assist during cyber conflicts to which they are not a belligerent is tied to the ideas of national responsibility or sovereignty and has been explored in the writings of Sean Kanuck (already referenced above) along with David Graham ("Cyber Threats and the Law of War" in the *Journal of National Security Law and Policy*, 2010) and Patrick Franzese ("Sovereignty in Cyberspace" in *Air Force Law Review*, 2009). These authors all have general consensus around certain points, such as (in Franzese's words), "Many of the designers of cyberspace viewed it as an intellectual nirvana free from the constraints of the 'real' world. In reality, however, cyberspace is part of the 'real' world and thus subject to its constraints and order—in other words, subject to state sovereignty."

More recently, a paper by this author explores the idea further and describes a ten point spectrum of national responsibility.[12] The present paper will apply and extend this spectrum to bring clarity and rigor to the idea of political neutrality in cyber conflict.

3. WHAT DO WE MEAN BY POLITICAL, VICE LEGAL, NEUTRALITY IN CYBER CONFLICT?

Even in the traditional domains of air, land, sea it may not be clear how to apply the Hague guarantee that "The territory of neutral Powers is inviolable." But in those domains neutrality is far clearer than in cyberspace.

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, criminal denial of service attacks, nuisance

10 *Ibid*., p. 1.

11 Joshua E. Kastenberg, "On-Intervention And Neutrality In Cyberspace: An Emerging Principle In The National Practice Of International Law," Air Force Law Review, Volume 64, 2009.

12 Jason Healey, "Beyond Attribution: Seeking National Responsibility in Cyberspace," Atlantic Council, 2012. Earlier published as "The Spectrum of National Responsibility for Cyberattacks" in the Brown Journal of World Affairs, 18.1 Fall/Winter 2011.

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 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. So far the world has only seen a subset of the likely kinds of cyber conflict. Modifying treaties to accommodate only those we have seen so far would be myopic and modifying them to include conflicts 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. For example, Russia is under no legal obligations to be impartial between the belligerents in the Syrian uprising, since it is not an international armed conflict. Despite this lack of legal standing, other nations can apply the political (that is, diplomatic) pressure of moral condemnation to convince Russia to cease shipping weapons to the Assad regime.

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, not by international tribunals, but heads of state and public opinion it establishes in essence a separate set of norms for international behavior.

The attacks against Estonia in 2007 provide a practical example of political neutrality in cyber conflict. Cyber attacks inundated Estonia during a political crisis between Estonia and Russia. The attackers followed "instructions provided on Russian-language Internet forums and websites," and were supported by comments from senior Russian politicians.[13] The attacks themselves appeared to originate from – or were routed through – 178 different countries. All of these countries which were asked, bar one, agreed to help cease the attacks and assist the Estonian investigation. The exception was Russia, which waited six weeks (indeed, after the conflict was over) to refusal, an act that "was not the inevitable legal solution, considering both earlier [Estonian] cooperation practice with Russia and the practice with other countries with whom identically phrased bilateral agreements."[14] Ever since, Russia has been presumed to have been, if not a legally defined belligerent, then at least complicit and iniquitous.

This then, is the heart of the political neutrality in a cyber conflict. Some nations certainly helped Estonia not to be impartial, but rather the opposite, to give them active assistance in the face of perceived bullying. Other nations, however, probably did indeed seek impartiality, choosing not to be a source of attack traffic tormenting a fellow nation during a crisis to which they were not a party.

Nations might (and probably *should*) come under political pressure to take reasonable steps to stop cyber attacks, regardless of whether or not it is a formal treaty obligation.

13 Eneken Tikk, et al, "International Cyber Incidents: Legal Considerations," NATO CCDCOE, 2010, p. 33.
14 *Ibid*., p. 27.

4. 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: "Does routing of attacks by a belligerent state through the internet nodes of a neutral country violate its neutrality?" as it was put by the ICRC.[15] 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" as such through those 178 nations in the way we normally think of a weapon system being routed. These attacks were not predominantly cyber missiles, launched from one the government of one belligerent and passing through the territory of other nations on its 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 country, or (2) been the location from which non-state patriot hackers launched such attacks in support of their original motherland.

Indeed, though being the source of attack traffic is the most visible way that nations can lose their political neutrality in a cyber conflict, it is not the only way. 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).

Note that, importantly, 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 based on a responsible 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.

15 Andrew Carswell, "Neutrality in Cyberwar," Presentation To The Internet In Bello: Seminar On Cyber War, Ethics & Policy, UC Berkeley School of Law, 2011, *available at* http://www.law.berkeley.edu/files/Neutrality_in_Cyber_War_for_web.pdf.

5. 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 Ruritanian leadership and the 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, though they are inconvenient. In response, Ruritania asks for assistance. Zendia and its client Trissalia unsurprisingly refuse to take any action; Floria attempts to stop the attacks but cannot, lacking technical and law enforcement capacity. Pollabia and Glospland are able to stop the attacks.

After the attacks continue for some weeks, pro-Ruritanian hackers both in that country and the diaspora, organize a sizable counteroffensive against Zendia using botnets in all the above countries. Ruritania asks these attacks to stop as they are "not helpful" to de-escalate the situation. Zendia requests help and again Floria tries to help but cannot. Trissalia, which had claimed it was unable to track down the hackers or computers involved in the operation against Ruritania, suddenly finds the ability to help Zendia. The attacks are rapidly stopped and Trissalia extradites those responsible to a gloomy fate in Zendia. Pollabia stops these attacks as effectively as it did for those against Ruritania. Glospland responds to the requests from Zendia, but still sends technical teams to Ruritania to bolster their defenses and provides emergency loans to buy advanced security kit.

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

Phase 2: Since Ruritania's defenses have become significantly better at blocking attack traffic, 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 massive (and noticeable) denial of service attacks using 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.

Ruritania feels that Trissalia and Floria, with attack teams on their own soil, these countries 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. It asks for help 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: nearly 200 people have been left dead and injured after the disruption of traffic lights, medical records, and local electrical power. Floria, which had been unable to stop the attacks earlier, realize the change in the nature of the conflict and are able to implement 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 Ruritania 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 and, 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.

6. UNDERSTANDING POLITICAL NEUTRALITY IN CYBER CONFLICTS

As noted in an earlier previous section 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[16] (see Table 1) is helpful – but not conclusive – to determine how each 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. The spectrum starts from a very passive responsibility—a nation having insecure systems that lead to an attack—up to very active responsibility—a national government actually planning and executing an attack. Countries that fall into the first two categories ("State Prohibited" and "State Prohibited But Inadequate") have only very passive responsibility – and are the most politically neutral – since they will, at the least, attempt to cease any participation in the attacks. In the next four categories ("State Ignored," "State Encouraged," "State Shaped," and "State Coordinated") the nation is in no sense neutral, as it is actively ignoring or abetting the attacks. In the final four categories ("State Ordered," "State Rogue Conducted," State Executed," and "State Integrated"), the state has a much more direct hand as a belligerent, either ordering attacks or conducting them itself.

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.

The spectrum can be used both to describe individual attacks or a campaign of related attacks, and is meant to be both for the operational cyber defenders ("*General, this attack against us is probably* state-ordered. *If we ask that nation for cooperation, they*

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

will not help us, and we will tip our hand.") and the policy community (*"The policy of our nation is to hold nations accountable for any* state-ordered *attacks as if those attacks were coming from the uniformed military services. You can't hide behind proxies."*).

The Spectrum of State Responsibility provides a much clearer vocabulary for political neutrality. Nations at the high end of the spectrum have more characteristics of a belligerent while those at the bottom end are the most neutral. Nations that take direct actions for one belligerent but not all of them, may be seen as helpful but not neutral.

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. **Ruritania** was also a belligerent, in that there were broad societal attacks, but it did try to rein in counterattacks. **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 to both parties, 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 Zendia as the party facing the online aggression.

At no point was "attribution" particularly important: indeed the applicable norms would prohibit supporting a conflict even if none of the belligerents are known. The attacks do not need to be traced to determine the computers and command and control network involved, then the people and organizations that were ultimately in control. The obvious attack traffic could have just been stopped, regardless of the geopolitical situation.

In the scenario, the technical community would try bottom-up technical attribution, but top-down attribution, would clearly point to Zendia as being to blame. The Zendian government would certainly try to hide behind the fiction that their involvement could not be "proved" but especially once there were casualties, this cover would have become increasingly threadbare.

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.[17]

- **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.
- **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.

17 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).

These important points often seem undervalued or even ignored in the current discussion which often focus on today's headlines on cyber crime and espionage – which are important but not severe. Accordingly, 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 attacks which are the most easily detected and stopped, as there is a higher obligation to stop these.

In the example above, Floria did not have the capacity to be as politically neutral as it would have liked. But it turned out this incapacity was conditional, and lasted only as long as the attacks were a crisis but not a catastrophe. Once there were hundreds of casualties, however, it felt a moral obligation (and probably a responsibility both to international and domestic audiences) to make strenuous efforts.

In the earliest phase, Ruritania was disappointed with the nations that failed to stop the attacks, especially those nations that did not even try. One reason was that denial of service attacks and botnets are fairly easy to both spot and stop. Internet Service Providers (and by extension, States) can typically spot this kind of traffic transiting their systems and there are methods to counter them. Ruritania was right to be upset by nations that could not reign in these attacks. By the later phases, some of the attacks had become "low and slow" and Ruritania no longer had such a high expectation.

As for duration, this notional example is far closer to the history of actual cyber conflicts, which are not won or lost "at the speed of light" as is often imagined. Though individual engagements can indeed be that quick, the conflicts themselves are usually months-long campaigns with repeated clashes.

7. COMMERCIAL NEUTRALITY

The dominant difference between conflict in cyberspace is not the speed of operations, nor the fuzziness of borders, or global reach. While important, these are dwarfed by the fact cyberspace is owned and operated overwhelmingly by the private sector. Any relevant national-security relevant conflict 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 governments 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 of the Packet Clearing House describes the long track record of successful

cooperation between the world's largest network providers to stop the most disruptive attacks.[18] 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 U.S. 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,' 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 needed to be involved.

In 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 (like AT&T, NTT, or BT) decided to suppress it?

8. CONCLUSION

Political neutrality will be an important norm for future cyber conflicts and this paper has examined the idea: what is it, past literature, and important and overlooked aspects. The central part of this paper developed a reasonable, but notional, scenario that explored how various nations would have different levels of neutrality, a determination helped by the ten-point scale of the Spectrum of National Responsibility.

Though the discussion of neutrality in cyber conflict started at least in 1999, with the DoD General Counsel paper, it seems to have made little headway until just the last few years. Further research should extend several of the ideas in this paper, including the difference between political and legal neutrality, the use of the Spectrum of State Responsibility, and include analyses that include the severity, obviousness, stoppability and duration of the attacks in question.

This paper introduced the importance of commercial neutrality, given the outsize role of the private sector in cyberspace. This area deserves much more research, indeed more than is given to exploring how the Hague and other treaties apply.

In future, States and others that see cyber conflicts, like those against Estonia in 2007, are unlikely to be able to sit back and say "not my problem" even as attacks transit their network.

18 William Woodcock, "The Next Fighting Force in Cyberspace," Conference on CyberFutures, Air Force Association, 23 March 2012.

When everyone is a neighbor in cyberspace, there will be no sidelines on which to sit. New norms, some backed with the force of international law, will come into the fore. These and other issues will become increasing important as the world sees more cyber conflicts and the researchers that study and predict it increase our understanding.