

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Cyber Conflicts in International Relations: Framework and Case Studies

Alexander Gamero-Garrido
Engineering Systems Division
Massachusetts Institute of Technology
gamero@mit.edu | agamerog.mit@gmail.com

Executive Summary

Overview

Although cyber conflict is no longer considered particularly unusual, significant uncertainties remain about the nature, scale, scope and other critical features of it. This study addresses a subset of these issues by developing an internally consistent framework and applying it to a series of 17 case studies. We present each case in terms of (a) its socio-political context, (b) technical features, (c) the outcome and inferences drawn in the sources examined. The profile of each case includes the actors, their actions, tools they used and power relationships, and the outcomes with inferences or observations. Our findings include:

- Cyberspace has brought in a number of new players – activists, shady government contractors – to international conflict, and traditional actors (notably states) have increasingly recognized the importance of the domain.
- The involvement of the private sector on cybersecurity ("cyber defense") has been critical: 16 out of the 17 cases studied involved the private sector either in attack or defense.
- All of the major international cyber conflicts presented here have been related to an ongoing conflict ("attack" or "war") in the physical domain.
- Rich industrialized countries with a highly developed ICT infrastructure are at a higher risk concerning cyber attacks.
- Distributed Denial of Service (DDoS) is by far the most common type of cyber attack.
- Air-gapped (not connected to the public Internet) networks have not been exempt from attacks.
- A perpetrator does not need highly specialized technical knowledge to intrude computer networks.
- The potential damage of a cyber strike is likely to continue increasing as the Internet expands.

- The size of the actor under attack could have an influence on its ability to deter the attackers with actions in the physical world.
- The entrance barriers (including the monetary cost) for any actor to get involved in a conflict seem to be much lower in the cyber domain than in the physical domain.
- Accountability on the Internet is difficult, and gets further obscured when the attacks transcend national borders. This fact has probably made cyber attacks desirable for major military powers such as China, Russia and the United States.

In many ways, this paper is a re-analysis of the case studies set presented on *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* recently published by the Atlantic Council. In addition, we draw upon other materials (academic and media) to expand our understanding of each case, and add several cases to the original collection resulting in a data set of 17 cyber conflict, spanning almost three decades (1985-2013). Cuckoo's Egg, Morris Worm, Solar Sunrise, Electronic Disturbance Theater, ILOVEYOU, Chinese Espionage, Estonia, Russo-Georgian war, Conficker, NSA-Snowden, WikiLeaks and Stuxnet are some of the major cases included.

Method And Organization

This study presents each case in terms of (a) its socio-political context, (b) technical features, (c) the outcome and inferences drawn in the sources examined. Emphasis is placed on characteristics of cyberspace visible on conflicts.

Present work is divided in several sections. Part I presents the cases in terms of the actors involved, their power relationship, main actions, layers of the Internet affected, and outcome. Part II expands on the tools and instruments used on the cyber offensive and defensive actions described on Part I, including an extended view of the layers of the Internet affected. Part III presents the author's inferences and observations for each case, highlighting features of cyber conflict. Part IV presents a set of conclusions highlighting critical features related to: actors, socio-political context, tools and other technical issues, sophistication of the attacks, outcome and damage, and accountability.

Countries Involved

Findings presented in this study are U.S.-centered, as this paper was developed using such a focus. However, 23 countries are involved in at least one case, either in attack or defense. Countries involved in two or more cases are (frequency in parenthesis): United States (16), Russia (7), China (3), Israel (3), The Netherlands (2) and Germany (2). Six of the cases presented had a global reach.



Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Cyber Conflicts in International Relations: Framework and Case Studies

Alexander Gamero-Garrido
Engineering Systems Division
Massachusetts Institute of Technology
gamero@mit.edu | agamerog.mit@gmail.com

Abstract

Twenty years ago, the possibility of having an international conflict extend into the cyber domain was distant. Since then much has changed. Today cyber conflict is not considered particularly unusual. But considerable uncertainties remain about the nature, scale, scope and other features of such conflicts. This paper addresses these issues using a re-analysis of the case studies presented in *A Fierce Domain* recently published by the Atlantic Council. In addition, we draw upon other materials (academic and media) to expand our understanding of each case, and add several cases to the original collection resulting in a data set of 17 cyber conflict, spanning almost three decades (1985-2013). Cuckoo's Egg, Morris Worm, Solar Sunrise, EDT, ILOVEYOU, Chinese Espionage, Estonia, Russo-Georgian war, Conficker, NSA-Snowden, WikiLeaks and Stuxnet are some of the major cases included. This study presents each case in terms of (a) its socio-political context, (b) technical features, (c) the outcome and inferences drawn in the sources examined. The profile of each case includes the actors, their actions, tools they used and power relationships, and the outcomes with inferences or observations. Emphasis is placed on characteristics of cyberspace visible on conflicts. Findings include: Distributed Denial of Service is the most common offensive action; accountability is difficult in cyberspace, particularly with international conflicts; outcomes of each instance have been variable, and economic impact is hard to estimate; the private sector has been a key player in cybersecurity; size of an actor, and countries' ICT infrastructure, influence the nature of the cyber conflicts.

Acknowledgement: This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.



Alexander Gamero-Garrido | Technology and Policy Program, MIT

The Underground Policy Fight Over The American Residential Internet

For millions of people around the world, the Internet is almost a necessity. We use it to communicate with our family, friends, employer, partners, random acquaintances, and virtually everyone we get in touch with. The Internet has become a platform for expression (political or otherwise), lust, friendship, anger, and an infinite spectrum of human emotions. Day after day we read stories of how the Internet is enabling forms of communication, economic exchanges, scientific development and so on. As a pervasive phenomenon, the Internet seems to be a very positive one.

For the average user (if not most users), the seamless operation of browsing through a website, using an iPhone app, or watching a TV show on Netflix is just that: a series of automatic responses to the commands given to the system. Such services, however, are not delivered by magic. Information is exchanged between us and our providers using networks. In the most simplistic terms, our computers are connected to an Internet Service Provider (ISP), and they connect us to the content we are trying to access (or transmit the information we want to upload). They allow us to watch web-based TV, browse, work, and have fun on the Internet. One could go as far as to say that ISPs *are* the Internet.

As the reader might infer, the story is not as simple. Internet's fluent operation is based on complex agreements among infrastructure owners (ISPs, transit providers, undersea cable operators), application providers (DSPs[1]), content delivery networks (CDNs), content owners, to name only the most salient ones. There are big, powerful corporations falling under each of

[1] Stands for Downstream Service Providers.

these categories, all looking to extract revenues from the American consumers. The infrastructure itself is also a puzzle of wires, pipes, technical protocols, radio communication towers, servers, and many other components.

I do not intend to describe the Internet in more detail, but it is not hard to see how this enormous, messy network can be a policymaker's nightmare. How do you regulate a network that is so poorly understood by most of its users? How can the government issue any policies pertaining a network that was built and is operated and serviced almost exclusively by private actors?

The Internet, however, did not emerge out of nowhere. ISPs consist mostly of cable TV and telephone providers, especially for residential users. With the advent of Voice over Internet Protocol (VoIP) and web video streaming, these companies faced a dilemma. On the one hand, they had clear incentives to block or degrade the performance of services that directly competed with their own offerings of traditional cable TV and telephone. On the other hand, their consumers demanded new applications, such as Netflix, YouTube, or Skype, to be delivered over the Internet for which they pay money every month. Other than protection of intellectual property, the regulation of this apparent conflict of interest has been the most important Internet policy controversy in recent times.

Network "Neutrality"

In the United States, the Federal Communication Commission (FCC) is the closest thing to an Internet regulatory agency. During the George W. Bush Administration, however, the FCC

decided that it would take a hands-off approach, and classified the Internet as an Information Service. By doing so, the FCC itself greatly restricted its regulatory authority over the Internet.

As more services move online, calls for regulation became increasingly frequent. One of FCC's responses to such calls was the 2010 Open Internet Report and Order (OIRO), which among other things prevented ISPs from blocking entire classes of Internet traffic (e.g. VoIP). In the words of the Commission: "broadband providers should not pick winners and losers on the Internet—even for reasons that may be independent of providers' competitive interests (…)."[2]

What did the commissioners mean by "pick[ing] winners and losers"? From a bird's eye view, they refer to a limited and valuable resource: residential bandwidth. In this context, bandwidth refers to the speed with which a connection can transmit information, and is normally measured in megabytes per second. It is the FCC's policy that it should be the consumer, and not the ISP, who selects how bandwidth should be allocated. Although this seems to point to a proposition of liberty (from ISP limitations), it is an argument about equity. Every consumer should have the right to select from her favorite service provider, and such provider should be allocated an equal portion of the available bandwidth on the ISP network.

As with Stone's chocolate cake[3], splitting bandwidth equally is not necessarily the fairest distribution. Specific applications such as VoIP are more time-sensitive than others, such as bulk-transfers[4]. ISPs, then, routinely have to prioritize entire classes of traffic over others. Since *you*, my theoretical neighbor, are having a telephone conversation that gets messed up if there

[2] Federal Communications Commission, "Preserving the Open Internet Broadband Industry Practices - Report and Order." 2010.
[3] Stone, D. "Policy Paradox." Third Edition. New York: Norton. 2012. Ch. 2.
[4] Buyya, R., Mukaddim, P., & Vakali, A.. Content Delivery Networks. Berlin: Springer. 2008

is a long delay, *I* might have to wait a few extra minutes to complete my Game of Thrones download, even though we both pay the same monthly fee for our Internet service. If later I decide to call my brother overseas using Skype, and you decide to download music, it is my traffic that will be prioritized. A grounded example of this treatment is the priority that ambulances, police and firefighter vehicles get when on duty: we, the rest of the drivers, recognize that they have a legitimate reason to be in a hurry and (usually) modify our behavior. We temporarily put their interests ahead of our own. In Stone's language this would be *unequal (Internet) traffic priority for equal traffic types.*

This form of discrimination is routinely used by ISPs to improve the performance of the network for all of their customers; this sounds like a legitimate policy. A perfectly neutral network would not allow for such discrimination. Are the operators, however, really looking to improve the performance of *every* service, including those competing with their own?

Network "openness"

In order to make VoIP and other delay-sensitive applications work, ISPs inspect residential traffic to prioritize such services. In this very act, proponents of neutrality argue, is embedded the possibility to harm competitors in an "unfair" way. Neutralers, as I will call the proponents of network neutrality regulation, claim that if the government does not regulate, ISPs will degrade the performance of competing services, especially video web streaming and telephony delivered over the Internet. It is precisely the providers of those downstream services, such as Google, who compose a big chunk of the neutralers. Their counterpart in the debate are the ISPs, particularly big ones such as Verizon or Comcast.

Although this seems to be a very technical discussion, proponents and antagonists of neutrality are really arguing about liberty versus control. Neutralers would like to see a very competitive market[5], where consumers can choose between many ISPs and, most importantly, get to decide what kind of classes are a priority for *themselves*. In a perfectly neutral world, it would be up to the user to choose their provider of Internet TV, VoIP, news, social networking or pornographic content. ISPs, neutralers continue, have no business in deciding what is a priority for all the Joe Smiths of America. There should be only minimal traffic control allowed, as to ensure minimal invasion of consumer liberty and protect offerings of competitive services. Comcast, neutralers argue, should not be capable of allocating a speedy lane to its own Xfinity web TV, to the harm of Netflix or Hulu.

We can all get behind this concept in theory. After all, the Internet has been infused with the values of its creator, the United States, which proclaims to be a beacon of liberty, openness and opportunity in the world. Neutralers, however, paint a picture of control that is very incomplete, and therefore misleading. In today's Internet, not all traffic is treated equally. Besides priority by traffic class, there are companies (CDNs) specialized in improving the performance of DSPs such as YouTube or Netflix. The latter pay big bucks to have their content delivered effectively to their subscribers. It is not only ISPs, then, who get to decide whose traffic is more important.

Neutralers would like to portray a picture where, as long as neutrality rules are enforced, over-the-top providers are all equal. CDNs and other mechanisms, however, ensure that if it is true

[5] Clark, *Vertical Integration on Access Networks (Personal Interview)*.

that all providers are equal, some providers are more equal than others[6]. There is no guarantee, then, that neutralers' call for regulation based on liberty and equity propositions are well grounded in reality.

Network "management"

Whether or not neutrality rules are enforced is not a matter of individual liberty. There are plenty of ways in which a consumer today is not making the backstage decisions that make some providers thrive and others succumb. Neutralers are, therefore, not defending Adam Smith's "invisible hand" of consumer choice over the "dictatorship" of ISP network management practices. Both sides agree that there must be some level of traffic discrimination for the Internet to continue shining. The fight is about *who* gets to control such traffic discrimination. This is a classic example of fighting over Harold Lasswell's "who gets what, when and how." It is a struggle for the right to control a process, a struggle for power.

ISPs claim that they have spent billions of dollars[7] building the physical infrastructure that allows the Internet to function. It is *their* network, they claim, and it is *them* who should be the gatekeepers of residential traffic. Should they not be able to recover their investments, the Internet in the United States will stagnate, since they will not build new pipes. The next ten million American users may never get to see a provider knocking on their door to offer them affordable Internet access, since such pipes will never reach their house.

[6] As in Orwell's *Animal Farm.*

[7] Watts et al., "Comments of AT&T Inc. Before the Federal Communications Commission." 2010.

As with many stories of decline[8] this one plays only half of the movie (the sad, doomy half). It conveniently leaves out that the Internet infrastructure was largely built on public land, under government concessions, and that therefore ISPs are not the "owners" of such a network[9]. They might own the wires, and they might have paid for digging the pipes. But to "own" the residential Internet is a very different thing, a much bigger ownership claim that does not stand minimal scrutiny. Firstly, ISPs accepted a great deal of control over their telephone and cable networks in exchange for building on public land[10]. Secondly, the Internet is much more than a "series of tubes"[11], as it relies on many protocols and soft tools that have been developed by the technical community, one that spans way beyond the ISPs themselves. Thirdly, and as with many infrastructures[12], there is much more to be extracted from the Internet than its simple data transmission capabilities.

As I argued in my opening paragraph, the Internet is now ubiquitous. It is hard to imagine living a modern life without the Internet. More than a nice thing to have, the Internet has become a necessity, and it greatly impacts the welfare (or the "well being") of the American people. To claim that the ISPs should be the *only* ones with a word to say about residential network management practices is to claim that ISPs have final ruling over welfare of its millions of users. It is effectively a call for a form of private government.

---

[8] Stone, D. See *supra* at 3. Ch. 7.
[9] Clark, see *supra* at 1.
[10] *Idem.*
[11] A congressman in the U.S. House of Representative famously coined this phrase.
[12] Frischmann, "Infrastructure Commons in Economic Perspective." 2008.

Closing Notes

Policy controversies surrounding network neutrality have been covered with a veil of technicalities and proxies that masquerade a fight over values. As such, what is at stake is much more than the revenue maximization of Comcast or Netflix[13]. It is the liberty, equity and welfare of the Internet: the most transformational technological development of the last century, with enormous consequences for the American way of living. I have not argued for or against neutrality rules myself, as my objective here was to show some of the underlying values that are being discussed. It is, however, one of the most challenging policy questions of this time, and we would all benefit from more clarity in the language of the proponents on either side.

[13] These two companies have been very active on the network neutrality debate, on opposing sides.