

Navigating the Internet's Unstable Terrain

James Cowie
Renesys Corporation

As military theorists grapple with the creation of suitable analogies and frameworks for understanding and responding to cyber threats, it's important to recognize the central importance of the Internet infrastructure, and the special challenges raised by its uniquely decentralized, trust-based operation.

The Internet's infrastructure --- the 'terrain' on which cyberwar is fought --- emerges from the voluntary technical collaboration of tens of thousands of independent constituent networks, establishing end-to-end reachability among hundreds of millions of individually addressable machines, in order to serve billions of users worldwide.

The mechanisms of collaboration that generate and maintain the Internet's complex terrain were designed solely to encourage distributed interoperation among cooperating networks. The Internet's design therefore maximizes the global infrastructure's growth and resilience by deliberately eliminating single points of failure and control, including centralized governmental oversight and regulation. Ironically, this attention to decentralization has left the Internet infrastructure vulnerable to certain kinds of trust-based attacks that manipulate the reality of the Internet's "terrain," since there is no centralized authority to consult for a determination of what is "real."

By manipulating the routing protocols that knit the Internet together, for example, it's possible for any well-connected network to impersonate any other network, claiming to be the legitimate originator of their assigned Internet addresses, thereby intercepting the Internet traffic destined for that network's users. The attacker may then elect to simply read the victim's traffic, impersonate the services normally provided by the victim, or even modify the traffic and return it, undetected, to its rightful destination (a "man in the middle" attack).

End-to-end encryption and authentication were brought in to support secure Internet communications atop this fundamentally untrustworthy global infrastructure, and on that basis, the modern Internet functions as an effective substrate for global civilization. However, the basic epistemological questions posed by the unreliability of the underlying infrastructure remain, and are a key source of complication for the establishment of a coherent theory of Internet defense and strategic operations.

The naming and routing infrastructures of the Internet are famously subject to attack and manipulation, and there are no globally deployable technical workarounds. If an attacker can redefine the very meaning of names, addresses, and paths on the Internet, they can destroy a defender's ability to accurately identify the owner and location of the resources used by an attacker. Worse yet, they can inject false information, leading the defender to specific false conclusions about attack attribution, in hopes of generating retaliation against a 'false flag' target.

Many of the very analogies on which early cybersecurity and cyberwar theories have been based --- the identification and establishment of defensible perimeters, the challenges of securing the national Internet, the desire to attribute actions to state actors based on the identity of the Internet resources used in an attack, the need to establish a credible deterrent force that can retaliate with speed and precision --- are brought into question, or at least made significantly more challenging, by the shifting nature of the reality of the underlying Internet infrastructure.

As a specific example of the kind of mischief that can be carried out, consider the recent "migration" of the Pirate Bay to North Korea. The Pirate Bay is a website that provides an index to the global pool of BitTorrent content, much of which violates the laws of jurisdictions where it is consumed. After years of legal pursuit by European governments, in March 2013 the site's operators announced that they had relocated their servers to friendlier territory: a datacenter in Pyongyang.

During the first days of the hoax, many Internet analysts were taken in by the story, which appeared legitimate, even under careful examination of the backing technical detail. The global routing table now contained apparently legitimate entries that seemed to show the Pirate Bay receiving Internet transit from North Korea's lone Internet provider, which in turn appeared to provide global connectivity through satellite provider Intelsat.

Running 'traceroute' (a common program for inspecting the raw IP-level connectivity along the path to a given Internet host) even displayed a sequence of hosts consistent with the North Korean story, and very high delays on one link, in excess of 500 milliseconds, consistent with the provision of services over a satellite in geostationary orbit. For all intents and purposes, the Pirate Bay servers had relocated to North Korea.

The only problem: none of it was true. By injecting false routes into the global routing table through their German provider, and by carefully replicating traceroute-visible delays that were consistent with satellite transmission, the Pirate Bay team created a *funkspiel* worthy of the best intelligence minds of WW2. The deception was nearly perfect, and was only revealed after careful examination of the delays experienced by specially crafted inspection traffic.

Such incidents demonstrate the necessity of carefully measuring the structure and performance of the global Internet, as a starting point for understanding the complexities of its operation. At a minimum, those who would support and defend the Internet's infrastructure need to understand the commercial and peering relationships among all the networks of the world, the geolocation of individual IP addressable resources, and the minute-to-minute interconnection and network performance of the paths taken by Internet traffic between arbitrary locations.

Even with this foundational intelligence at their fingertips, however, potential defenders must realize the fundamental limitations of any model for understanding the Internet's complex operations, and avoid jumping to conclusions based on preliminary intelligence. Any doctrine for escalation or retaliation that

assumes the existence of ground truth about the identity and attribution of specific Internet resources risks trivial manipulation by more sophisticated forces.

This lack of ground truth poses a special challenge to the well-connected countries of the Americas and Western Europe, where the Internet is freely available at low cost, and commonly perceived to be a utility with the same stability, predictability, and reliability as the power grid or water supply. Westerners tend to deal with complexity by creating models, and then trusting those models, often far beyond their reasonable point of applicability.

Elsewhere in the world, by contrast, generations of children are growing up with the opposite Internet experience. In their world, Internet consumers are technically sophisticated information consumers, cognizant of how traffic flows and how it can be controlled, familiar with the use of Internet proxies, encryption, and the tools of anonymity. Access to the Internet is never taken for granted; it's negotiated, and continually reassessed in light of the shifting political and security environment. By learning to regard the Internet as an adversarial environment where nothing is certain, or easy, the residents of emerging Internet markets will have a clear advantage in navigating the uncertain terrain of the 21st century Internet.