# WHEN GOOD METAPHORS GO BAD: The Metaphoric "Branding" of Cyberspace

## Adriane Lapointe*

Current cybersecurity discussions rely heavily on imaginative metaphors, models, and related rhetorical devices which initially provide insight into the challenges we face in cyberspace, but too often end up as empty labels or catch phrases used by different people to mean different things. When metaphors begin to function in this way, they can become an impediment to meaningful discussion rather than a vehicle for creative thought. This paper looks at how some of the most common cyber metaphors currently shape our discourse, considering the extent to which they do or don't contribute to a clearer vision of our way ahead, and why.

❖◆❖◆❖

Metaphor has obvious appeal for people thinking about cybersecurity and other aspects of cyberspace. Metaphors and analogies emphasize relevant similarities, offer insight into complex issues, and give us ways to talk about new things or situations which are hard to grasp more literally. Because a relatively simple metaphor can sometimes convey the gist of a complicated idea, metaphor is ideally suited to describe the complexities of cyberspace.[1]

But of course no metaphor can provide the whole of the literal "truth" about the topic it describes. Metaphors and analogies are by definition true *to a certain extent*; they do not correspond with absolute fidelity to the thing itself—a fact we may know in principle, but

[1] And of course cyberspace is itself a sort of metaphor. Unless we are talking about the literal physical location of hardware, cyberspace is not an actual physical space available for high-tech exploration, like outer space, but rather more like the space between our ears, a conceptual arena in which we "move" around and accomplish things by "visiting" or "going to" sites, among other things, without physically leaving our living rooms, offices, or command centers. The fact that we tend to think of cyberspace as a space we can move through or inhabit reflects the extent to which we "place" ourselves within it, the extent to which we perceive ourselves as located within the system rather than as looking on at its operation from a distance. The equation of "virtual worlds" and "virtual meeting spaces" with physical space is so natural to many of us that it is perhaps harder to remember the metaphoric nature of this "space" than it is to accept it as a literal description. For an interesting discussion of cyberspace as a metaphor, see Raymond Gozzi, Jr., "The Free Library by Farlex," July 1994, http://www.thefreelibrary.com/The+cyberspace+metaphor.-a015543199.

can easily lose sight of in practice. And by focusing our attention on one particular aspect of a subject, metaphors can limit our thinking as easily as they can broaden it. An apt metaphor or analogy is useful, then, as long as we remember that it shows us only facets of the truth, and as long as we are attentive to the point at which a given facet ceases to reflect light on the situation.[2]

**The Cyber Ecosystem Metaphor**

The idea that a set of network technologies, or of network technology customers, can be metaphorically described as an "ecosystem" is probably the most prominent cyber metaphor in wide use today. The metaphor goes back at least to the early 2000s in the context of IT marketing, probably inspired by the "business ecosystem model" introduced in the early 1990s by James F. Moore.[3] As of 2011, industry continues to use the ecosystem model to sell hardware and software, but the metaphor has also been adopted by people writing or talking about cyber policy issues ranging from the pros and cons of net neutrality to the best approaches to cybersecurity.[4]

The ecosystem metaphor can be applied to cyberspace in a number of different ways. It implies complex interconnection and functional interdependency, but an ecosystem is hardly the only, or perhaps even the most obvious, model for interdependency between diverse entities. Consider, for instance, the idea of the internet as a symphony orchestra, each section playing a different part, but all sections working together to produce a literally harmonious result. On its face, this is a reasonable model of successful and complex interrelationship between diverse entities, but it's not really apt as a model of cyberspace. An orchestra is a more or less rigid structure: members of the orchestra interact based on a pre-existing score, and are kept in line by a conductor. If someone with a newly-

---

[2] For the purposes of this paper, metaphor includes notional models and analogies; for a seminal discussion of metaphor defined in this way, see George Lakoff and Mark Johnson, *Metaphors We Live By*, Chicago, University of Chicago Press, 1980.

[3] See http://www.provenmodels.com/574_and http://en.wikipedia.org/wiki/Business_ecosystem. We cannot, of course, rule out the possibility of convergent evolution. For an excellent account of the related "network" metaphor, see the first chapter of Richard R. John's *Network Nation: Inventing American Telecommunications*, Cambridge, MA: Harvard University Press, 2010.

[4] Just a few examples of the use of cyberspace/internet-as-ecosystem include "Internet Ecosystem and FCC's Net Neutrality Proceeding," Tom Tauke, Verizon Policy Blog, April 26, 2010.http://policyblog.verizon.com/BlogPost/725/InternetEcosystemandFCCsNetNeutralityProceeding.aspx; "The Internet Ecosystem: The Potential for Discrimination," Dirk Grunwald. http://www.law.indiana.edu/fclj/pubs/v63/no2/Vol.63-2_2011-Mar._Art.-04_Grunwald.pdf; "Ten Years in the Evolution of the Internet Ecosystem," Amough Dhamdhere, Constantine Dovrolis. http://www.cc.gatech.edu/~dovrolis/Papers/internet-evolution-imc08.pdf; "Enabling Distributed Security in Cyberspace," Department of Homeland Security, March 23, 2011. http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

invented instrument wandered onto the stage mid-performance, it would not be immediately obvious how to fit him or her into the score, or even where s/he should be seated. The orchestra metaphor emphasizes centralized control and fixed structures, which are not traits we associate with cyberspace.

Unlike a symphony orchestra, an ecosystem will accommodate a new entity (although the "accommodation" might consist of killing it off) and will change in response to shifts in the environment. This suggests that the ecosystem metaphor is illuminating as much because it implies the ability to accommodate change in some more or less "automatic" way as it emphasizes interconnection and interdependency.

Several papers on the idea of technological ecosystems from the last decade are quite explicit about the centrality of this "adaptive" aspect. "An Ecosystem Model of Technology Evolution" (2004) begins by defining an ecosystem as a "habitat for a variety of different species that co-exist, influence each other, and are affected by a variety of external forces (such as climate changes and natural disasters)," a habitat in which "the evolution of one species in an ecosystem affects and is affected by the evolution of other species." The paper goes on to describe the relationship between "social and technological forces" as symbiotic, observing that each drives change in the other.[5]

The paper "Information Technology Ecosystem Health and Performance" (2005) describes the IT ecosystem as a "network of organizations that drives the creation and delivery of information technology products and services," and stresses that "[l]ike its biological counterparts, the IT ecosystem is characterized by a large number of participants who depend on each other for their mutual effectiveness and survival."[6]
Consistent with the business thrust of their paper, the authors posit "three aspects of the [sic] ecosystem health inspired by our biological metaphor and expressed in terms of our ecosystem analogy: robustness, productivity, and innovation (or niche creation)."

---

[5] "An Ecosystem Model of Technology Evolution," Gediminas Adomavicius, et al., 2004. http://misrc.umn.edu/workingpapers/fullpapers/2004/0429_112404.pdf.
[6] "Information Technology Ecosystem Health and Performance," Marco Iansiti and Gregory L. Richards, 2005. http://www.hbs.edu/research/pdf/06-034.pdf. See also "Towards a Wi-Fi Ecosystem: Technology Integration and Emerging Service Models," Vinoth Gunasekaran and Fotios C. Harmantzis, 2005. http://howe.stevens.edu/fileadmin/Files/publications/Towards_a_Wi-Fi_Ecosystem.pdf; and the interesting "A Digital Ecosystem in Jordan: October 2002," James F. Moore, 2002. http://cyber.law.harvard.edu/is03/Readings/Moore_Jordan_Oct_2002.pdf. The last paper expands the notion of digital ecosystem to include not just technology, but communities of people and a relatively wide range of human activities. Professor Moore describes "positive sum relationships" as "symbiosis."

It's easy enough to see how the ecosystem metaphor works in this economic context: some IT companies compete with each other, directly affecting each other's bottom lines, spurring innovation or precipitating decline. Other IT companies work more "symbiotically," benefiting from, or supporting each other's work. Some segments of the market don't touch others directly, but influence them through intermediaries or by shaping the market as a whole.

While high-level discussions frequently characterize the IT business marketplace as a single overarching ecosystem composed of member businesses or even sectors, the IT sector is also represented as consisting of multiple ecosystems. These ecosystems may be composed of the companies competing or collaborating in a given market, e.g., the "mobile ecosystem," "apps ecosystem," "location ecosystem," "smartphone ecosystem," and "[Facebook] Platform ecosystem." [7] Alternatively, IT ecosystems may be conceived of as groups of companies which cooperate in providing support to a given product; this second kind of ecosystem could be considered a subset of the first.[8] Another potentially related use of the term refers to a particular company's network.[9] All these ecosystems are defined and made coherent by the goals of the members and the nature of the "environment"—that is, the specific market segment—in which they operate, with market forces serving as a rough stand-in for natural selection.

Some references to a "cyber ecosystem" are really just references to this IT model. But another version of the cyber ecosystem is quite different, both by virtue of its much broader scope, and because the ecosystem it posits is not the product of economic forces. The best-known and most fully articulated example of this non-economic "cyber ecosystem" concept is laid out in the DHS-sponsored white paper, "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action."[10] As in the papers cited earlier, the ecosystem metaphor

---

[7] Testimony presented at the Hearing on Protection and Privacy in the Mobile Marketplace, Senate Commerce, Science and Transportation Subcommittee on Consumer Protection, Product Safety, and Insurance, May 19, 2011.
[8] E.g., Microsoft's "robust partner ecosystem," "Microsoft Announces Partner Ecosystem to Lead Media and Entertainment Industry to the Cloud," April 12, 2011. http://www.microsoft.com/Presspass/press/2011/apr11/04-12MSNAB2011PR.mspx?rss_fdn=Press%20Releases. See also "What is an Ecosystem?" Invensys Operations Management, 2011. http://iom.invensys.com/EN/Pages/IOM_WhatIsAnEcosystem.aspx, and "Nokia, Microsoft Form Mobile Ecosystem Partnership," Forbes.com, April 21, 2011. http://www.dtic.mil/whs/directives/corres/pdf/510020p.pdf.
[9] The term "network ecosystem," as it refers to the range of products and services that make up the network owned/operated by an individual company or other entity, is bounded simply by ownership of the network rather than by dynamic market forces, but it is focused on entities created and supported by the market. Dmitri Alperovitch, quoted in "Enter the Cyber-dragon," Michael Joseph Gross, *Vanity Fair*. August 2, 2011. http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109?printable=true#ixzz1TyAz9gvk.
[10] "Enabling Distributed Security in Cyberspace, pg. 2") Characterization of the internet as a single, comprehensive ecosystem dates much earlier than this paper, but the concept has become much more common recently.

functions here as an ideal model of interconnection and automatic adaptation, with the emphasis on the speed with which the adaptation occurs.[11]

The DHS white paper explicitly defines "the cyber ecosystem [as comprising] a variety of diverse participants – private firms, nonprofits, governments, individuals, processes, and cyber devices (computers, software, and communications technologies) – that interact for multiple purposes." This definition not only includes all flavors of IT ecosystem, but explicitly identifies the ecosystem concept as including "devices" and "processes" as members. Defined in this way, the term "cyber ecosystem" is a conveniently all-encompassing label, a quick way to convey the cross-category breadth and diversity of cyberspace and cyber entities in two words. The value of such a term is obvious to anyone who's had to come up with a not-too-long, but sufficiently representative list of internet constituents more than once in a discussion.

As with metaphors generally, this strength can also be a weakness, depending on how it's used. Unlike even a singular, overarching IT ecosystem, whose members may or may not interact significantly, but are at least subject to similar economic forces, the internet itself may be the only point of connection between the members of this vast cyber ecosystem. A category so broadly defined that it includes people, electrons, and everything in between is rather like the category "things on earth": useful as a label, but not likely to tell us anything very substantive about the relationship between any two members.

As one commentator noted with regard to a recent Senate committee hearing—at which "there were so many references to the 'ecosystem' that [he] felt like [he] had stumbled upon an Environment Committee hearing by mistake"— the decision to use an ecosystem metaphor which casts all of cyberspace/internet as a single, intimately interconnected community implies relationships that may or may not exist. Regardless of whether one agrees with the article's overall argument, it's hard to disagree with its observation that for many purposes "it is important to draw some lines, rather than lumping all players together into a big, undifferentiated [cyber] 'ecosystem.' "[12]

The increasingly popular notion of "cyber ecosystem health," also popularized by the DHS white paper, is currently the most prominent variation on the cyber ecosystem metaphor. As it turns out, the idea that even real biological ecosystems can be "healthy" is metaphoric in origin: a 2001 paper on biological ecosystem health notes that part of the

---

[11] By way of contrast, the 2003 *National Strategy to Secure Cyberspace* emphasizes speed of response, but not adaptivity, by characterizing cyberspace as the country's nervous system . http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf, p. vii.

[12] David Sohn, "COICA and the Internet 'Ecosystem'," Center for Democracy and Technology, February 16, 2011. http://www.cdt.org/blogs/david-sohn/coica-and-internet-ecosystem. This short article is an excellent discussion of a specific instance in which choice of metaphor shapes and limits thinking about a complex issue.

appeal of the idea of ecosystem health "is that it appears to be a simple, straightforward, intuitive metaphor . . . [a]pplying the notion of human health to ecosystems."[13] Biological ecosystem health depends not on the health of specific members, but rather on the overall ability of the system to survive and cope with change. "An ecological system is healthy . . . if it is stable and sustainable—that is, if it is active and maintains its organization and autonomy over time and is resilient to stress."[14] If we accept this definition, the internet, the highly resilient system that it is, would seem to be very healthy indeed.

Linking the idea of cyber ecosystem health to cybersecurity is more problematic. The 2011 DHS white paper postulates "a healthy, resilient—and fundamentally more secure—cyber ecosystem of the future, in which cyber participants, including cyber devices, are able to work together in near-real time to anticipate and prevent cyber attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state."[15] The goal is of course ideal, but the ecosystem metaphor may not do it full justice. Biological ecosystems can be stable and resilient, but are they *secure*? The idea that the "health" of cyberspace depends on the exclusion or suppression of selected members is not necessarily consistent with the notion of an ecosystem. However happy it might make the gazelle, we don't imagine that we'd make the savanna ecosystem "healthier" by taking the lions out of the Serengeti. Ecosystems are value neutral—predators can contribute every bit as much to the system's stability and resiliency as their prey—and this makes them problematic metaphors for a vision of the internet focused on cybersecurity.[16]

Given that the original concept of biological ecosystem "health" was intended to help policymakers with environmental policy decisions, it is perhaps unsurprising that cyber ecosystem health, and the yet more popular cyber ecosystem root metaphor, have gained considerable currency in policymaking circles.[17] At a recent Congressional hearing, for

---

[13] "Values, Policy, and Ecosystem Health," Robert T. Lackey, 2001. http://www.epa.gov/wed/pages/staff/lackey/pubs/values.pdf. This interesting article discusses the implications of the concept of "ecosystem health" in some detail.

[14] "What is Ecosystem Health and Why Should We Worry About It?" Benjamin D. Haskell, *et al. Ecosystem Health: New Goals for Environmental Management*, 1992. p. 9. http://books.google.com/books?hl=en&lr=&id=opzqx56nBkMC&oi=fnd&pg=PR9&dq=ecosystem+health&ots=4upTGQ3VWh&sig=T_hsMTyrA2SVDyAeJgvHcL-Nyrg#v=onepage&q&f=false.

[15] "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action."

[16] Unlike the idea of eliminating predators from an ecosystem, the idea of protecting ecosystems from external threats like invasive species might make more metaphoric sense in a cyber context. This version of the metaphor might be worth pursuing—or it might not. What's important is not how far we can extend, or how cleverly we can construct a metaphor, but how much insight it provides and the extent to which it helps us communicate effectively.

[17] Lackey, 2001.

instance, the phrase "cyber ecosystem" was used 11 times.[18] At the hearing referred to earlier in this paper, it was used 14 times.[19] Over the past two years, at a range of House and Senate hearings, it was used more than 150 times. [20]

But as already suggested, the term doesn't always mean quite the same thing, even within a single hearing. In some instances the cyber ecosystem whose health we wish to promote consists of the entire internet and all its constituents—human, technical, and electrical—explicitly consistent with the DHS white paper discussion.[21] In other instances—as with the proposal that we "address cybersecurity both at the level of the entire ecosystem and also within specific sectors" –the cyber ecosystem seems to be a collection of organizations, many of them sector members, possibly defined in economic terms.[22] In many other hearings, the term refers to the kinds of IT ecosystem constructs described earlier. The point here is simply that "cyber ecosystem" is a protean concept: the ecosystem is in the eye of the beholder.[23]

The extent to which versions of the ecosystem metaphor pervade our cyber discourse suggests that it has attractions that go beyond the convenience of a term that stresses the diversity or interrelationship of cyber constituents. The flexibility of the term is probably part of the charm. The familiarity of the concept, based on its use in business generally

---

[18] The Committee on House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, CQ Congressional Testimony, June 24, 2011.
[19] Hearing of the Senate Judiciary Committee on Targeting Websites Dedicated to Stealing American Intellectual Property. February 16, 2011. *CQ Congressional Testimony.*
[20] This figure was arrived at after a case by case review of hits on the term "cyber ecosystem" in a LexisNexis search of *CQ Congressional Testimony* for the years 2010 and 2011. Hearings reviewed included: Hearing of the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee of the House Homeland Security Committee, June 24, 2011; Hearing of the Senate Judiciary Committee, June 22, 2011; Hearing of the Communications and Technology Subcommittee of the House Energy and Commerce Committee, June 22, 2011; Hearing on Cybersecurity and Data Protection in the Financial Sector, Senate Banking, Housing, and Urban Affairs Committee, June 21, 2011; Hearing of the Crime and Terrorism Subcommittee of the Senate Judiciary Committee on Cybersecurity, June 21, 2011; Hearing of the House Oversight and Government Reform Committee on Federal Spending Transparency and Accountability, June 14, 2011; Hearing of the Communications and Technology Subcommittee of the House Energy and Commerce Committee on Commercial Special Auctions, June 1, (2011; Hearing of the Intellectual Property, Competition and the Internet Subcommittee of the House Judiciary Committee, June 1, 2011; Hearing of the Communications and Technology Subcommittee of the House Energy and Commerce Committee, May 25, 2011; and so on . . .
[21] Testimony Before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technology. Statement of Melissa Hathaway, CQ Congressional Testimony, June 24, 2011. http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Hathaway.pdf.
[22] Testimony Before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technology. Statement of Leigh Williams, CQ Congressional Testimony, June 24, 2011.
[23] In this respect, the cyber ecosystem metaphor presents a challenge similar to that of the term "cyber" itself, though on a smaller scale. As many have observed, the "cyber" metaphor—or perhaps rather the "cyber" brandname—us applied so broadly that it's often difficult to determine which of the many possible versions or aspects of cyberspace of this internet is being addressed. This challenge obviously deserves more than a footnote's worth of attention.

and then in IT specifically, is obviously another factor. But another possible explanation could be the positive connotation, among much of the public, of the prefix "eco" followed by anything short of "terrorist." Characterization of the internet as an ecosystem could be a kind of benign "greenwash," rebranding cyberspace as a living environment-cum-organism deserving of conservation and care—a notion particularly consistent with the idea of "cyber ecosystem health."[24] Cyber ecosystem is an easy phrase to like: it's green, non-threatening, and agnostic about responsibility: we can all be part of it. It rolls off the tongue as easily as the redundant "safe" does before "haven," and therein lies the rub. However thoughtfully they may be used at the outset, terms like this can rapidly become catch phrases which pad out sentences, express broad generalities, or simply mean something specific to the speaker but vague to everyone else.

**Cyberspace and Public Health Metaphor**

Many of the images linking cyberspace with different aspects of human (as opposed to ecosystem) health have become so familiar as to be more or less transparent; how many of us really think about contagion or the co-opting of a cell's reproductive mechanism when we talk about computer "viruses," or about biological modes of transmission when we casually refer to a computer as "infected"? But of course images like these were originally vivid and effective ways of explaining how some malware works to computer owners who were less likely then than now to understand a more literal explanation of malicious executable code.[25]

Biological metaphors, developed into models, have not only helped make complex processes or relationships easier to grasp, but have in some instances directly inspired technical innovation: computer science-related examples include genetic algorithms, and evolutionary programming.[26] The fact that biological models have on more than one occasion in the past led creative individuals to new and even "disruptive" ways of doing things may encourage belief that biological metaphor in the cyber world could provide the same kind of actionable, problem-solving insight in this new context.

The human health/infectious diseases metaphor has certainly been plumbed for this kind of concrete guidance. Discussions of computer "hygiene" as a means of preventing the spread of "infection" go back at least to 2007, but hygiene is well on its way to becoming

---

[24] The neologism "greenwash," green + whitewash, is properly applied to deliberate efforts to conceal environmentally damaging aspects of a product or activity with eco-friendly packaging, advertising, etc.
[25] These are examples of "dead metaphor," metaphor which no longer conjures up a comparison between two things, though the term may retain connotations associated with the original comparison.
[26] As a jumping off point, see "genetic algorithm," *Wikipedia*. http://en.wikipedia.org/wiki/Genetic_algorithm. "Evolutionary programming," Scholarpedia.org,. http://www.scholarpedia.org/article/Evolutionary_programming.

as dead a metaphor as the notion of infection itself: the most common use of the term is as the headline for a list of security best practices for home computers.[27]

The "Internet Health Model," a 2010 Microsoft paper that draws an analogy between action taken by the CDC to prevent mass outbreak of infectious disease and the kinds of actions that could be taken to stem the spread of malware, uses health system and infectious disease metaphors to justify possible restrictions on internet access for users who become metaphorically contagious, as a means of protecting the wider community of internet users.[28] This metaphor is interesting in more than one way. Like any good metaphor, it invites us to consider illuminating similarities between two overtly dissimilar things—malware on the internet and infectious disease in a community—similarities that can lead us to reframe a familiar topic. It also identifies a policy precedent, reminding us that we do, as a society, recognize the need to impose some restrictions on individuals who involuntarily pose a certain kind of threat to others, and that we have a mechanism to do this which might be relevant to cybersecurity matters. Whether we ultimately decide that this mechanism or approach is appropriate to the cyber challenge, the metaphor has certainly helped to broaden thinking about the subject.

Another common health-related metaphor compares the cybersecurity mechanisms we want for the future to the human immune system. This metaphor extends the much older virus and infection metaphors, and suggests immediate, unreflecting, constructive, self-regulating response to intrusions. It's hard to imagine much disagreement with the idea that a network security architecture which functions like the human immune system would make the internet dramatically more secure than it is today (although the metaphor might also lead us to think about things like autoimmune diseases). The comparison is vivid, and certainly gives the non-technical a sense of the speed and efficiency with which an automated security framework could operate.

---

[27] See, for instance, "National Cybersecurity Awareness Advocates Good 'Cyber Hygiene'," CIO.gov. http://www.cio.gov/pages.cfm/page/National-Cybersecurity-Awareness-Month-Advocates-Good-Cyber-Hygiene.

[28] Scott Charney, "Collective Defense: Applying Public Health Models to the Internet," 2010. http://download.microsoft.com/download/7/F/B/7FB2F266-7914-4174-BBEF-2F5687882A93/Collective%20Defense%20-%20Applying%20Global%20Health%20Models%20to%20the%20Internet.pdf. Deirdre K. Mulligan and Fred B. Schneider devote a substantial part of their paper, "Doctrine for Cybersecurity," to a discussion of this aspect of the public health model. May 15, 2011. http://www.cs.cornell.edu/fbs/publications/publicCybersecDaed.pdf. For an earlier use of the CDC metaphormodel, see Joe St Sauver, "We Need A Cyber CDC or a Cyber World Health Organization," Anti-Phishing Working Group Counter e-Crime Summitt, May 31, 2007. http://pages.uoregon.edu/joe/ecrime-summit/ecrime-summit.pdf.

Unlike the CDC metaphor, however, it doesn't suggest a precedent or imply a way ahead: comparisons of internet traffic filters to mast cells and mucus, or of detection and early warning to smell and taste, may strike us as clever or interesting, but at least as currently presented, they don't provide insight into how new filtering or detection mechanisms might be designed.[29] This limitation doesn't render the metaphor useless, but it does raise the question of whether extending a given metaphor truly advances our case or simply distracts us from it.

**Cyberspace as Battlefield**

Although biological cyber metaphor is very much in fashion, it is by no means the only kind of metaphor prominent in discussions of cybersecurity today. In a statement on cybersecurity to the National Press Club on December 17th, 2010, Secretary of Homeland Security Janet Napolitano called attention to a couple of what she described as competing analogies—what we are calling metaphor—for cyberspace as she stressed the importance of partnerships both within and outside government to cybersecurity.

[There] are some who say that cybersecurity should be left to the market. The market will take care of it, and there are some who characterize the Internet as a battlefield on which we are fighting a war. So it's the market or the war. Those are the two analogies you hear. . . In my view, cyberspace is fundamentally a civilian space, and government has a role to help protect it, in partnership with responsible partners across the economy and across the globe.[30]

The reference to the market is not really so much an analogy as a description of where some people believe responsibility for cybersecurity lies. The metaphor "cyberspace is a battlefield on which we are fighting a war" is linked to the opinion (which context makes clear the Secretary does not hold) that cyberspace is more appropriately protected by military rather than by civilian entities. As used elsewhere, the same phrase can also reflect concern about what is sometimes referred to rather diffusely as the "militarization" of cyberspace. These are issues we will return to.

But to start, let us note that the "internet battlefield" metaphor is frequently used in discussion of issues unrelated to war: it's used to characterize such diverse things as cyber crime, conflict over value systems, efforts to win civil liberties or the right to free

---

[29] "Enabling Distributed Security in Cyberspace," p. 9.
[30] *Newsroom Magazine* USA Edition, December 28, 2010. http://newsroom-magazine.com/tag/national-cyber-incident-response-plan/.

expression, use of the internet for targeted abuse, and competition within the IT industry.[31] Even an article with a title like "Cyber-Security's New Global Battlefield: U.S., Russia, China" turns out to be about diplomacy, and not military conflict at all.[32] The term "battlefield" is a common metaphor for a situation in which individuals "fight" (argue, disagree, conflict) and may be "wounded," perhaps even grievously, in a non-physical, sometimes purely emotional sense.

This non-military version of the battlefield metaphor is perhaps most useful with regard to cyberspace as it reflects the fact that life online is somewhat dangerous, that there are always "bad actors" waiting to do something to you. If we look at the way cyber criminals increase the sophistication of their exploits every time cybersecurity and cybercrime professionals find countermeasures to existing techniques, it's easy to slide further into the language of metaphoric war and talk about "escalation." The common phrase "cyber attack," used to describe aggressive behavior ranging from a DDoS event to a targeted

---

[31] See, for example, the paper soft, 2005. http://download.microsoft.com/download/b/5/6/b566cdf9-a3d5-43a3-b756-7d23e34be7d8/battlefield.doc. This particular paper uses the metaphor quite consciously, keeping both "battlefield" and "tactics" in quotation marks. Another example is "War rages on internet battlefield," Electronic Payments International, www.vrlknolwedgebank.com, October 2008. https://encrypted.google.com/url?sa=t&rct=j&q=war%20rages%20on%20internet%20battlefield&source=web&cd=1&sqi=2&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.commercemedia.net%2Fdocuments%2Fuploads%2Fnews_articles%2FEPI_-_War_rages_on_the_Internet_Battlefield_2.pdf&ei=kz9qTroBguDRAc_FkPgE&usg=AFQjCNHJ2n9_c3-XOkAF5FZzM47mUzTTnQ&cad=rja. Here the internet is colorfully described as the "hunting ground of cyber-criminals"—bring on the hounds. Examples of cyberspace as a battlefield for conflict over values include "In the Shadow of Innovation," Gaia Bernstein, 2010. http://www.law.stanford.edu/display/images/dynamic/events_media/In_the_Shadow_Innovation_Bernstein.pdf. The "Internet Battlefield" section of this paper addresses conflicts between "openists," proponents of open and decentralized internet structure, and "centralists" who believe in control and "propertization" of the internet (p. 16). Another example is "Scientology Unmasked: Church, enemies wage war on Internet battlefield," Joseph Mallia, *Boston Herald*, March 4, 1998. For a battlefield on which to the fights is over civil liberties or free expression, see the following three articles: "China: the Internet as an ideology battlefield," Global Voices Advocacy, January 6th, 2010. http://advocacy.globalvoicesonline.org/2010/01/06/china-internet-as-an-ideology-battlefield/. "Battlefield Internet: Belarusian civil society active despite censorship," Pavel P. Antonov, Association for Progressive Communications, April 2, 2008. http://www.apc.org/en/news/battlefield-internet-belarusian-civil-society-acti. "Internet a Battlefield in Egypt" by Jesse Emspak, *International Business Times*, January 26, 2011. http://www.ibtimes.com/articles/105506/20110126/internet-a-battlefield-in-egypt.htm. For use of the battlefield metaphor in the context of targeted abuse on the internet: "Mayfield students step into Internet battlefield," *The Tidings.com*, March 4, 2011. http://www2.the-tidings.com/2011/030411/cyber.htm. For cyberspace as a personal battlefield, see "Cyberbullying on the Rise, on Campus," Edward A. Brown, *Bostonia*. http://www.bu.edu/bostonia/web/cyberbullying/. The article opens with the observation, "Cyberbullying: it's not just a teenage battlefield any more." And for the cyber battlefield as a site of competition, see this ad for mobile microprocessors: "Mobile Microprocessors: Industry Titans Collide on the Mobile Internet Battlefield" (reference to internet gaming). In-Stat, http://www.instat.com/promos/09/IN0904636WHT.asp.

[32] "IT Security & Network Security News & Reviews: Cyber-Security's New Global Battlefield: U.S., Russia, China," Brian Prince, *eWEEK*.com, November 23rd, 2010. http://www.eweek.com/c/a/SecurityCyberSecuritys-New-Global-Battlefield-US-Russia-China-332374/. The article addresses claims that China "hijacked" internet traffic in 2010.

intrusion into private systems, fits neatly into the idea of a battlefield distinct from actual war.[33]

While this non-military cyberspace-as-battlefield metaphor may be practically irresistible on occasion, only the most hardcore security experts—or hackers—would argue that it conveys the whole of our experience on the internet. One rather trivial inconsistency is the fact that battlefields generally involve two-way combat; we may fire up our anti-virus programs to protect ourselves, but those of us who are not hackers are unlikely to go head to head with criminal aggressors. More important, even colloquial discussion of cyberspace as a battlefield shifts our focus away from the myriad useful, profitable, and enjoyable aspects of life on the internet.

This brings us back to use of the battlefield metaphor by those with actual military activity in mind. Not surprisingly, many references to a cyber battlefield are relatively literal references to an actual physical battlefield on which cyber technology is being used.[34] References to the cyberspace or the internet as "battlefield" also turn up frequently in the titles of articles/blogs addressing the standup or operations of US CYBERCOMMAND. In many of these cases, the "battlefield" is mentioned only in the title, and does not inform the actual discussion, which is to say that the word is present to signal military

---

[33] Military and international relations cyber experts understandably object to the use of the word "attack" in this context, arguing that it should be reserved for instances associated with the possibility of real, death-dealing war, and their desire to establish at least local clarity with regard to the meaning of terms like attack is reflected in calls for a cyber lexicon. There are many good things to say about such an undertaking--cyber policymakers need to be sure that they understand what other cyber policymakers are talking about--but any effort to specialize common terms to suit the needs of a particular group runs at least a couple of risks: first, that it will narrow participation to a circle of cognoscenti who know the lexicon, shutting others out, and second, that those who rely on the specialized meanings will find themselves with a "domain" problem—that is, that the terminology they use with the best of intentions will be misinterpreted by, or will simply baffle, non-experts (read: most internet users) who come into contact with it. The standardization of non-standard meanings for common terms within the DoD, for instance, almost certainly simplifies activities internally, but it does not make those activities transparent to people outside the Department. In the end, the linguistic convenience of the few has seldom had much affect on the way language is used by the many, and the impulse to describe what Lulz Security did to Sony as an attack is unlikely to fade. "LulzSec Releases Sony Usernames, Passwords," Hayley Tsukayama. *Washington Post*, June 2, 2011. http://www.washingtonpost.com/blogs/post-tech/post/lulzsec-releases-sony-usernames-passwords/2011/06/02/AGY4zWHH_blog.html

[34] See, for example, "US Cyber-Combat Needs Rules," David A. Fulghum, *Military.com*, March 23, 2010. http://www.military.com/features/0,15240,212587,00.html; and Deputy Secretary of Defense William Lynn's statement that "protecting military networks is crucial to the Defense Department's success on the battlefield," "U.S. Cyber Command: Waging War in The World's Fifth Battlespace," Rick Rozoff, Media Freedom Intl, May 27, 2010. http://www.mediafreedominternational.org/2010/05/30/u-s-cyber-command-waging-war-in-the-worlds-fifth-battlespace/. An interesting historical perspective is provided in "Battlefield Internet gets first war use," David Rising, Associated Press, April 16, 2003. http://www.msnbc.msn.com/id/3078666/ns/technology_and_science-science/. Back in 2003, a "digitized [Army] division" used a computer network to guide battlefield equipment like tanks.

involvement rather than to illuminate the relationship between military activity and cyberspace.[35]

To return to Secretary Napolitano's remarks, it is clear that she used the "cyberspace as battlefield" metaphor not in the ways described above, but because she was interested in what entity (the Department of Defense or Department of Homeland Security, in this case) should be relied upon to protect cyberspace. In this context, the phrase "cyberspace is a battlefield" is less a mechanism for providing insight into the nature of cyberspace than convenient shorthand for a regime in which the military would serve as the primary government provider of cybersecurity.

As another metaphoric reference to military involvement with cyberspace, the phrase "militarization of the internet" is worth brief mention here. This phrase is among the fuzziest of the metaphoric characterizations of cyberspace/internet in common use, first, because the precise literal meaning of "militarization" is a bit shifty, and second, because the one entirely sure thing about the word is its negative connotation.[36] To "militarize" is to give something a military character or style, to provide military equipment, or to establish a military presence. In some instances, the term is applied to cyber issues in just this way, with the idea, for instance, that packets used to achieve military goals in cyberspace are the equivalent of bullets, or of soldiers on the ground.[37] But the phrase "militarization of cyberspace" is more typically used with less precision, serving as a placeholder for a

---

[35] For instance, see "Pentagon's Cyber Command seeks authority to expand its battlefield," Ellen Nakashima, *Washington Post,* November 6, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507304.html; "US creates military command for cyber battlefield," Dan De Luce, Google News, June 23, 2009. http://www.google.com/hostednews/afp/article/ALeqM5jotOynJlC4Z123ZHZU-TdBPJ34zw.

[36] A review of dictionaries will provide a wide range of definitions of "militarize" and "militarization." The negative connotation of "militarization" probably derives in no small part from that of "militarism," which denotes a glorification of military ideals or even the control of a state by its military. The point here is that when the term is used, the thoughtful reader/listener is required to determine what the author means by it from some quick analysis of the rest of the argument. The interpretive work required by a good metaphor is constructive to the extent that it leads us to look for and understand similarities and differences; the kind of analysis we have to do to grasp the precise meaning of "militarization" is frequently more like the kind of analysis we must bring to bear on a poorly written sentence. The use of the word can be a bit like much popular use of the word "socialism"—the point is less what it means than what is for many its negative connotation.

[37] See, for instance, Richard Clarke's "Software Power: cyber warfare is the risky new frontline," February 7, 2011 http://www.powerandpolicy.com/2011/02/07/software-power-cyber-warfare-is-the-risky-new-frontline/. Talking about US CYBERCOMMAND and the development by other countries of cyber-specific military resources, he notes that "America is not alone in militarizing cyberspace," equating militarization to the stand up of military entities that use "software applications as their weapons" in order to counter other militaries or compromise civilian infrastructure.

range of concerns or different kinds of negative sentiment rather than providing focused insight into specific aspects of the intersection between military activity and cyberspace.[38]

**Cyber Commons and Cyberspace as a Domain**

Discussion of cyberspace in terms of physical space both reflects and encourages the notion that it can be either circumscribed and dominated or kept open and free, notions we see embodied in what are perhaps the most enduring cyber metaphors, cyberspace as a "domain," and the internet as a "global commons."[39] Both concepts draw a comparison with land from the perspective of ownership and access; the difference between the two is who is doing (or not doing) the owning and who can have access.

The term domain is strongly associated with sovereignty, and clearly implies ownership. The second of the two common current meanings of the word—an area of expertise or activity—was once a metaphoric extension of the core meaning, an area owned or controlled by a particular ruler or government. The word's oldest meaning, that of land belonging to a lord, informs the word's connotation even today.[40] Domains are not the purview of ordinary people: a man's home may have been his castle from time immemorial, but the average person has never been likely to refer with a straight face to his or her backyard as a "domain." Domains are things not only owned, but dominated—the root of the words is of course the same—by an overarching power.

Because domains are always somebody's turf, ownership or control of a domain can be defended or contested. It is presumably for this reason that the word domain was originally adopted by the military to describe the physical dimensions of the world which

---

[38] Some anti-militarization critiques equate "militarization" with geopolitical conflict broadly, and with domestic censorship and surveillance. Examples include "Militarizing Cyberspace," Ronald Deibert, *MIT Technology Review*, July/August 2010. http://www.technologyreview.com/computing/25570/; "Political Cyberattacks to Militarize the Web," Fred O'Connor, IDG News, PCWorld Business Center, March 12, 2009. http://www.pcworld.com/businesscenter/article/161142/political_cyberattacks_to_militarize_the_web.html); and "Cyberwar," Fault Lines, Al JazeeraEnglish, April 23, 2010. http://www.youtube.com/watch?v=ciAqopNRL0U&feature=player_embedded#at=1310. In addition to expressing concern about militarization of the internet, the Al Jazeera report includes a short but intriguing discussion of war as a metaphor for response to cyber threats: "The US government's reaction to the challenge [of cybersecurity] is guided by a metaphor: that of war…it's a simple way of translating technical, people [sic], and cultural complexities for a broad audience. But metaphors can become reality, and in the fog of war, facts get hidden and right are taken away. So is war the right metaphor?"

[39] The prevalence of special metaphor in discussions about cyberspace –once more important to this paper --- is outlined by Thomas Karas, Judy H. Moore, and Lori K. Parrott in "Metaphors for Cyber Security". Sandia Report, August 2008. http://evolutionofcomputing.org/Multicellular/Cyberfest%20Report.pdf The paper also identifies the same rough categories of cyber metaphor touched on here.

[40] See the historical *Oxford English Dictionary (OED)* entry for "domain."

are capable of defense and "in" which wars can be fought. The Armed Services currently uses the term "domain" in a relatively neutral sense to refer to the different physical environments for which the Services must "man, train, and equip."[41]

Although military reference to land, sea, and air as "domains" attracts little attention, military use of the phrase "cyber domain" does not fall in a neutral way on civilian ears.[42] There are of course real and substantive issues with, and concerns about the nature and scope of potential military activities in cyberspace, but reflexive use by the military of the word domain, with its "overlord" connotations, particularly in conjunction with phrases like "cyber dominance," may have generated unease in and of itself.[43]

The idea of the internet as a commons is, as far as anything associated with such a recent phenomenon can be, a venerable one. Early usage referred to land usable for some purpose by all members of a community, and is in this sense rather like the notion of right of way as it still exists in England; a field belongs to someone, but a right of way may cut across it, allowing free passage in spite of private ownership.[44] The commons metaphor conceives of the internet as a communally-held space, one which it is specifically inappropriate for any single individual or subset of the community (including governments) to own or control. The internet is compared to a landscape which can be used in various ways by a wide range of people for whatever purpose they please, so long as their actions do not interfere with the actions of others. Like a domain, a commons can be fenced in, and it can be defended, but the defense and fencing would be to very different ends: a

---

[41] "Domain" is not officially defined in the authoritative DoD military glossary Joint Publication 1-02 separately from the areas with which it is associated (e.g., air domain is defined, but domain is not). The Joint Publication defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (CJCS CM-0363-08)." Joint Publication 1-02, "Department of Defense Military and Associated Terms ," as amended through July 15th, 2011. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, p. 91-92.

[42] A representative article on the release of DoD's cyber strategy entitled "Pentagon to treat cyberspace as an 'operational domain'" gives greater play to the fact that cyberspace has been designated a domain than to the Deputy Secretary of Defense's discussion of the military's specific cyber missions. David Alexander, "Pentagon to treat cyberspace as an 'operational domain,'" *Reuters*, Thursday, July 14, 2011. http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714.

[43] In a non-military context the use of the term "domain" in the context of "domain names" suggests the relationship between a set of distinct name "spaces," little fiefdoms associated with different governing (assigning) authorities. In this realm, too, one sees battles for control and a feeling on the part of some entities that they have been rendered powerless by an overlord.

[44] See the full historical *Oxford English Dictionary (OED)* entries for "commonty, "commonage," and "commons." References to "common of pasture" go back to 1540; use of related language to describe lands held in common, as distinct from land privately owned, dates back to at least 1600.

commons is fenced or defended to stave off those who would exert individual ownership or control over it, in order to keep it free to all comers.[45]

The domain and the commons metaphors are essentially mirror images, both envisioning cyberspace as a kind of vast, bounded territory, but one focused on ownership or control of the territory, and the other on what it would regard as the preservation of that territory's peculiar freedom from control. Each reflects the particular overarching governance principle its users espouse, much as political party affiliation might reflect an individual's values.

Although the domain and commons metaphors succinctly imply a general attitude toward cyber governance, they are less useful when they are bounced up against the heterogeneous reality of information technology. Control is sometimes exercised; authoritarian governments have made intense and sometimes effective efforts to control at least aspects of the internet. But even in these cases, dominance is less than complete and enduring, and the impulse to censorship seems often to be smoke to the fire of what insecure governments perceive as dangerous independence on the part of their "netizens."[46] Efforts on the part of ruling elements to flat-out "switch off the internet" within their domains, while highly problematic, have not lasted long, and have not been entirely successful while in effect.[47]

Conversely, how can the cyber commons be regarded as genuinely free when governments exercise *any* kind of coercive control over access at their geographical borders, or require IT providers operating on their soil to censor or manipulate internet operations? The policies and business decisions of the companies that own and operate internet sites and services also circumscribe users' cyber freedom of choice and of action. Access to "free" information or services, for instance, not infrequently require consumers to pay for access with personal information, and some sites will sell products and services

---

[45] For a good discussion of, among other things, the way in which cyberspace is "not . . . outer space, but . . . a real world physical space," see Jeff Strabone, "What Kind of Space is Cyberspace?" *3 Quarks Daily*, September 7, 2009. http://www.3quarksdaily.com/3quarksdaily/2009/09/what-kind-of-space-is-cyberspace.html.

[46] See "China sets up office for Internet information management," *Xinhua*, May 4, 2011. http://news.xinhuanet.com/english2010/china/2011-05/04/c_13857911.htm. On the tendency of an authoritarian government to see independent activity on the internet as threatening, see "Micro-blogging, a good thing is bad," Li Hongmei, *People's Daily Online*, February 22, 2011. http://english.peopledaily.com.cn/90002/96417/7296323.html.

[47] The Egyptian government's restriction of Internet access lasted 5 days. "Egypt reverses 'kill switch' to restore Internet access," Gregg Keizer, *ComputerWorld*, February 2, 2011. http://www.computerworld.com/s/article/9207803/Egypt_reverses_kill_switch_to_restore_Internet_access. As *The Economist* notes, "[t]he more complex communications networks become, the harder it is to disable them swiftly, remotely or unilaterally." "Reaching for the Kill Switch," *The Economist*, February 10, 2011. http://www.economist.com/node/18112043.

only to those willing to create accounts which allow the vendor to retain credit card numbers and other information under security conditions unknown to the consumer.

We should not be surprised, of course, that no single metaphor is likely to cover the two trickiest aspects of internet governance: the fact that the actual infrastructure is in the main commercially owned and operated, and the fact that the infrastructure is inevitably located in a physical space owned and operated by some government. In the end, the high-level principles these metaphors express do more to remind us of what's at stake or to reflect our general desires or world view, than to give us practical insight into how internet governance might actually work.

**When Good Metaphors Go Bad: Metaphoric "Branding"**

The question with which this paper began was how thinking and reasoning in terms of cyber metaphor affects our efforts to secure cyberspace for the nation—and indeed, for the world more generally. The answer is in one way very simple: any one of the metaphors discussed can illuminate or obfuscate, depending upon how thoughtfully and aptly it is employed. This much we knew from the start.

Metaphors are useful as ways to explain complex topics. A good metaphor's strengths, however, are also its weaknesses: a metaphor which grabs us because it seems especially apt can also restrict our thinking by framing the discussion so effectively that we fail to question our vantage point. We may even forget that we have a limited vantage point, that we are in fact talking metaphorically rather than literally.

This is the classic caution offered to those who might be seduced by metaphor. But while this caution certainly applies, there are at least two other drawbacks to our enthusiasm for cyber metaphors which merit attention. The first of these is the readiness of many who read or hear them to adopt them uncritically and use them less as metaphors than as brand names for vague and overarching concepts. When this happens, metaphors which may initially have "captured the imagination" end up making no demands on the imagination at all. The best example of this right now is the increasing prevalence of references to the "cyber ecosystem"—references which less and less frequently evoke the insights that gave the metaphor value.

When metaphors become nothing but labels, buzz words, or catch phrases, they not only lose their power to provoke thought or offer insight, but in the worst cases allow us to refer to our subject without thinking precisely about what we mean. This is most problematic

when discussion is substantive and such portmanteau phrases are allowed to stand in for thoughtfully drawn distinctions and solid explanations.

And this brings us to the second problem with undue reliance on metaphor: it is possible to expect metaphoric language to do too much. Metaphor has borne a heavy burden in public discourse on cybersecurity. Because cyberspace is variously a physical network; the traffic flowing through that network; social sites, business transactions, and so many other things, any given metaphor could be applied in many different ways. If we use metaphors without a precise meaning in mind, and without making that context clear to our audience, we do so at our own risk.

Metaphors give us useful insights into cyberspace, but we cannot reasonably rely on metaphors to give us insight into the entirety of the challenge the internet offers us. The more undifferentiated aspects of the internet a metaphor is intended to cover, the greater the likelihood that it will come, over time, to seem more literal than metaphoric, and either circumscribe our thinking or—more likely—dwindle to little more than an empty catch phrase. When these things happen, an originally useful metaphor no longer contributes to constructive debate, and may even complicate it.

Consider the common characterizations of the United States as the “great melting pot” or “a city upon a hill.” Think both about the specific meaning and context of each—what aspects of the U.S. each stresses—and think, too, about the many issues to which they are utterly irrelevant. It would be a considerable stretch to say that these metaphors are relevant to decisions about physical infrastructure or tax rates, but they could figure productively in a discussion of some aspects of immigration or foreign policy. No one would look to either as a guide for the totality of U.S. policy. In the same way, we would be unwise to expect any one cyber metaphor—or indeed, any group of cyber metaphors—to guide us to the best cybersecurity or overall cyber policies. It is unquestionably tempting to approach cyberspace, with its great technical, social, commercial, national security, and intellectual complexity, in figurative terms, but substantive discussion of the way ahead depends on our ability to leaven our literal discourse with a dash of metaphor rather than the other way around.