Wolff, Josephine

Article

What we talk about when we talk about cybersecurity: security in internet governance debates

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Wolff, Josephine (2016) : What we talk about when we talk about cybersecurity: security in internet governance debates, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 5, Iss. 3, pp. 1-13, https://doi.org/10.14763/2016.3.430

This Version is available at:
https://hdl.handle.net/10419/214025

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 5 | Issue 3

What we talk about when we talk about cybersecurity: security in internet governance debates

Josephine Wolff
Department of public policy, Rochester Institute of Technology, United States, jcwgpt@rit.edu

Published on 30 Sep 2016 | DOI: 10.14763/2016.3.430

Abstract: At meetings of internet governance organisations, participants generally agree that improving security is an important goal, but these conversations rarely yield consensus around how to achieve this outcome. One reason security plays this paradoxical role—as both a universal point of agreement and a continued source of contention—in these debates is that it has significantly different meanings to different stakeholders involved in these governance forums. In this paper, we discuss how different stakeholders define and frame internet security issues in the context of governance debates and analyse how these conflicting notions of security continue to shape emerging controversies.

Keywords: Cybersecurity, Internet governance, Internet Corporation for Assigned Names and Numbers (ICANN), WCIT

Article information

Received: 25 Apr 2016 **Reviewed:** 17 Jun 2016 **Published:** 30 Sep 2016

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/what-we-talk-about-when-we-talk-about-cybersecurity-security-internet-governance

Citation: Wolff, J. (2016). What we talk about when we talk about cybersecurity: security in internet governance debates. *Internet Policy Review*, *5*(3). DOI: 10.14763/2016.3.430

This paper is part of Doing internet governance, a special issue of Internet Policy Review *guest-edited by Dmitry Epstein, Christian Katzenbach, and Francesca Musiani.*

INTRODUCTION

"Despite widespread use of 'security' by scholars and politicians during the last forty years, not much attention has been devoted to explicating the concept," Baldwin (1997) argues in his discussion of security as an ambiguous and inadequately explored idea. While the problem of "security" being insufficiently explicated may seem largely academic and theoretical, the lack of

clarity surrounding this term has become of significant and immediate practical importance among the participants vying for control in the multistakeholder forums of internet governance. This paper explores how the ambiguous nature of security, discussed and debated in the literature of security studies, is amplified and enacted in current discussions of online security due to the multistakeholder model of internet governance.

Security has been a recurring theme in the ongoing debates about internet governance, especially as a tool for national governments seeking to claim greater authority in the multistakeholder system. In preparation for the December 2012 World Conference on International Telecommunications (WCIT), for instance, several nations submitted proposals to revise the International Telecommunications Regulations (ITRs) treaty to include more language about security. These changes were intended to broaden the treaty's scope and, accordingly, to expand the purview of the United Nations International Telecommunication Union (ITU), which convened the WCIT, to include issues related to internet security. The previous version of the ITRs, negotiated and signed in 1988, did not make any mention of telecommunications security, but the most recently revised ITRs, signed by 89 nations at the 2012 WCIT, make several references to security, including a new article on the "security and robustness of networks" (International Telecommunication Regulations, 2012).

The broad language about security used in the ITRs does not clarify what it would mean to ensure the security and robustness of networks, much less how governments ought to go about doing this. This confusion in the realm of internet security is not unique to international governance bodies—many actors, from private firms to individual government agencies, have far-reaching and ambiguous definitions of their roles in contributing to online security. However, in the evolving and controversial internet governance landscape the ambiguity and conflation of security issues is especially striking because everyone in attendance at internet governance meetings is generally willing to agree that improving security is an important goal for the internet, but these conversations rarely yield much consensus about how to achieve this outcome. This is not a new phenomenon; Wolfers (1952) points out that "The term 'security' covers a range of goals so wide that highly divergent policies can be interpreted as policies of security". But the broad diversity of participant groups that the multistakeholder model specifically seeks to foster can exacerbate this problem. Having many different stakeholders at the table in such forums, each with their own goals and notions of security, can contribute to even greater divergence around ideas of security than in more traditional governance models.

This paper considers conflicting constructions of security by stakeholders in three cases of internet governance controversies: the proposals to the ITU to enable states to restrict how their internet traffic is routed addressed at the 2012 WCIT, the debate over the creation of dot-less domains within the Internet Corporation for Assigned Names and Numbers (ICANN), and the ICANN discussions of revising the WHOIS policy governing the privacy of domain registration information. For each of these cases, we explore how the underlying controversies were cast as "security" issues by parties on all sides of the debates, and how each stakeholder group's different perspective on what constituted a secure internet shaped their use of security-related rhetoric. Finally, we discuss how these conflicting notions of security continue to shape emerging controversies in the internet governance space and serve to abstract some of the sharpest differences in opinion between stakeholder groups by conflating several very different definitions of security into a single, shared vocabulary that represents several incompatible visions for what a more secure internet should look like.

SECTION 1: DEFINITIONAL ISSUES IN SECURITY STUDIES AND INFORMATION SECURITY

The challenges associated with defining security predate computers and discussions of cybersecurity. The field of security studies has long engaged with related questions, dating back to Wolfers' (1952) work on the nature of national security as an "ambiguous symbol". He argued, "the term 'security' covers a range of goals so wide that highly divergent policies can be interpreted as policies of security". Others in the field have suggested that the notion of security may be an "essentially contested concept", an idea "so value-laden that no amount of argument or evidence can ever lead to agreement on a single version as the correct or standard use" (Baldwin, 1997). Still others have traced a gradual broadening in the definitions of security over time to include greater emphasis on individuals, private organisations, international systems—not just nation states (Rothschild, 1995).

As the ongoing discussions around these issues would suggest, there are multiple definitions of national security even within the field of security studies. For instance, Wolfers (1952) defines a nation as secure "to the extent to which it is not in danger of having to sacrifice core values, if it wishes to avoid war, and is able, if challenged, to maintain them by victory in such a war". Ullman (1983), in an effort to provide a definition that also covers the potential for non-military threats to security, such as natural disasters, offers a variation on Wolfers' definition in which a threat to national security is defined more generally as:

> An action or sequence of events that (1) threatens drastically and over a relatively brief span of time to degrade the quality of life for the inhabitants of a state, or (2) threatens significantly to narrow the range of policy choices available to the government of a state or to private, nongovernmental entities (persons, groups, corporations) within the state.

The common thread in these definitions is the ability to maintain the status quo of a nation's government, values, and population.

Definitions of security drawn from the field of computer science and information security echo some of this same emphasis on maintaining the status quo (in a technical system, rather than a nation state) but in a notably different manner. The best-known and most widespread framework for information security is the "CIA triad", the notion that a network is secure when the confidentiality, integrity, and availability of its information are assured. This definition is commonly used in technical contexts, such as ISO 17799, an Information Security Management Standard published by the International Organization for Standardization (ISO), and the United States National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, to define the high-level goals of information security. However, it has also been criticised as incomplete, and other concepts, including authentication, non-repudiation, and control are sometimes added to this initial list of three (Beautement & Pym, 2010). For instance, the ISO and International Electrotechnical Commission (IEC) publication 7498-2, "Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture", defines the crucial elements of security for information processing systems as identification and authentication, access control, data integrity, data confidentiality, data

availability, auditability, and non-repudiation. Parker (1998) also expands on the CIA triad by adding utility, authenticity, and possession to his definition of a secure computer system. Another influential definition of security among technical stakeholders and engineers holds that a computer is secure only “if you can depend on it and its software to behave as you expect” (Garfinkel & Spafford, 2003). This definition lends itself to an interpretation of security wherein technical mechanisms are not manipulated or interfered with in unpredictable ways, but does not speak at all to the question of social consequences or harms that might result from security lapses, or even what specific characteristics—such as confidentiality, integrity, and availability, for instance—a computer system should be expected to exhibit.

The disagreements within the security studies community and the technical community about the appropriate definitions of security are not insignificant, but they pale in comparison to the differences across these communities. Definitions of national security, like those proposed by Wolfers and Ullman, emphasise the ability to resist change. Technical definitions of information security focus instead on the positive attributes a computer system must exhibit to be considered secure rather than the absence of threats or dramatic changes. The specificity of technical definitions of security also distinguishes them from definitions of national security, in part because information security definitions have a much smaller scope—they are confined by the boundaries of a computer system, rather than the boundaries of a nation. Cavelty (2010) points out that the apparent parallels between definitions of national security and information security can be misleading, writing, "The terminology in information security is often seemingly congruent with the terminology in national security discourses: it is about threats, agents, vulnerabilities, etc. However, the terms have very specific meanings so that seemingly clear analogies must be used with care". Nowhere is the care required to move back and forth between discussions of information security and national security more critical than in the multistakeholder forums that bring together the different stakeholders that espouse each of these very different views of security. In the context of these organisations, the definitional differences around security are not just theoretical—they lead to very concrete disputes as these distinct definitions collide in a single forum.

SECTION 2: SECURITY AND THE MULTISTAKEHOLDER MODEL

Existing literature has examined closely the notion of "multistakeholder" governance model of many internet governance forums such as ICANN and the IGF (Mueller, 2010; DeNardis, 2014). One consequence of the multistakeholder models espoused by these organisations is that each stakeholder group has its own distinct ideas and perspectives on how the internet should function and what desirable outcomes for its future would be. There is perhaps no area of governance where these views diverge more starkly than the realm of security. Notably, stakeholder groups involved in internet governance, including government officials, representatives of private industry, and members of civil society, don’t just disagree on what steps should be taken to help secure the internet—they also disagree on what it would mean to have a secure internet in the first place.

Private industry stakeholders, many of whom represent technical firms, tend to hold a view of security closest to that of the technical computer science definition, seeking to build systems that operate as expected, with strong protections for confidentiality, integrity, and availability. For government representatives and political stakeholders, the scope of the system they aim to

control (and protect) is much broader, so security is less likely to be focused on whether computers behave as expected and more likely to mean protection of a country's core values and status quo. For these stakeholders, a secure internet or computer is, correspondingly, more likely to be one that cannot easily be used to cause harm to people or governments. For many government stakeholders, definitional differences and nuances are disappearing as the notion of internet security is increasingly used as a proxy for national security (DeNardis, 2014). Meanwhile, civil society representatives, and especially political activists, engaged in internet governance forums often present their concerns about security as issues of personal and individual security, tied to anonymity and privacy protections, rather than national or technical security. Their notion of a secure internet is one in which it is difficult for governments—or corporations, or indeed, anyone—to identify online users' real identities.

Even within these stakeholder-specific definitions, all members of a given stakeholder group do not always agree about what constitutes a secure internet or how it is best achieved. National governments have different views, for example, on whether empowering a government to shut down internet connectivity within its borders, in emergency circumstances, would provide more or less security to their citizens. These differences speak to the strong political implications of the definition of security adopted by individual stakeholders, and the extent to which the security actions a group or government would most like to see taken often give rise to the definition they promote—rather than the other way around.

Because consensus building is such a crucial component of multistakeholder internet governance processes, however, these differences of opinion are largely hidden through use of broad language about "security" that effectively abstracts any concrete controversies underlying the general principles. Wolfers (1952) identifies this phenomenon in the field of security, more generally, writing that, "while appearing to offer guidance and a basis for broad consensus [notions like national security] may be permitting everyone to label whatever policy he favors with an attractive and possibly deceptive name". For example, Article 5A of the revised ITRs states that "Member States shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks". This language appears to foster cooperation among the member nations of the ITU by articulating a principle most governments feel comfortable affirming, but it does so not by disambiguating the ideas of network security and robustness, but rather by abstracting the ideas of security and robustness so there is sufficient ambiguity for every signatory to interpret those words according to their own opinions and priorities. Thus, security facilitates superficial cooperation among different stakeholders up to a point, without forcing them to confront the profound differences of opinion underlying their different interpretations of what a secure internet would look like, who and what it would be secure from, and who and what it would be secure for.

The security studies literature makes clear that using ambiguous definitions of security to foster superficial consensus is not new or unique to online security and internet governance. However, the multistakeholder model of governance is particularly susceptible to these problems given its emphasis on bringing together representatives of different segments of society and consensus building processes. In this context, participants start out often having very different views on issues and are then encouraged—even pressured—to find areas of common ground for controversial issues, leading to considerable variation in how they may frame and define those issues (Epstein, Ross, & Baumer, 2014). Mueller (2010) notes that "in internet governance, the term security now encompasses a host of problems, perhaps too many to fit properly under one word."

SECTION 3: METHODOLOGY AND CASE SELECTION

The approach taken in this paper to elucidate how the multistakeholder model exacerbates definitional differences in the meaning of security across different communities is a series of three case studies, presented chronologically: proposals to enable greater national control of internet routing at WCIT in 2012, proposals to create a dotless search domain through ICANN in 2013, and proposals to alter WHOIS database policies, debated at ICANN in 2015. Each case is analysed through the lens of how participants characterise the central issues as relating to security concerns in the documents, proposals, and statements they file related to the case. The analysis of individual cases based on close reading of formal documents touches on only a small portion of the security debates in the internet governance arena and is intended to offer a starting point for further, more thorough discussion of and research into these issues.

The corpus of documents analysed included working drafts of policy statements produced by these multistakeholder forums, as well as formal written comments addressed to these forums in response to policy proposals, and finalised statements of policy that resulted from these deliberations. Since each governance group has a different process for producing policy and soliciting comment, access to these documents varied; 18 documents were analysed for the WCIT case, nine for the dotless domains case, and 13 for the WHOIS case. ICANN makes all policies and comments publicly available on its website, while the ITU operates in a more closed fashion, only publishing the final, signed version of the ITRs. However, there were sufficient leaks of draft proposals and public commentary and response in the lead up to the 2012 WCIT that it was still possible to assemble a significant corpus of documents. References to security in these documents were analysed and coded according to which stakeholders they indicated being secured and which types of threats they indicated those stakeholders would be protected from.

By focusing on cases that centre on very specific, concrete changes to existing internet infrastructure, this analysis aims to ground the very broad, often vague discussions of security that are common to internet governance forums in the clearer, actionable proposals that force stakeholders to confront their differences in definition, giving rise to real disagreements. The cases were selected to highlight the clashes in opinions about security across the three primary groups of stakeholders involved in internet governance: governments, private industry, and civil society. Each case centres on a conflict between two of those groups: the internet routing case highlights differences in opinion between government representatives and private industry, the dotless domain case illustrates differences between private industry and civil society in conceptions of security, and the WHOIS database proposal is a case of government ideas about national security conflict with civil society's conceptions of individual security. Although the ITU, unlike ICANN, is not a multistakeholder forum, in the sense that only government delegations were permitted to vote at the WCIT, it is used in the presented case study as an instance of private industry conflict with national governments because the delegations from governments opposing the routing proposal were heavily populated by industry representatives who, in many cases, led the opposition to these proposals. For instance, the US delegation to WCIT consisted of 95 people, 60 of whom came from private industry and other non-governmental organisations, including Amazon, AT&T, Cisco, Facebook, Google, Microsoft, and Verizon. In fact, the fights at the WCIT around security in part stemmed from the decision by such nations to model their national delegations on miniature multistakeholder forums, even in the context of an explicitly governmental organisation.

SECTION 4: INTERNET TRAFFIC ROUTING PROPOSALS AT WCIT

The ITU, which convenes the WCIT, is not a multistakeholder body, but neither is it a body that has traditionally considered security to be within the scope of its mission to "enable the growth and sustained development of telecommunications and information networks, and to facilitate universal access so that people everywhere can participate in, and benefit from, the emerging information society and global economy". However, as a governmental governance organisation it is perhaps not surprising that the ITU chose security as one of the linchpins of its effort to claim authority in internet governance issues. Ensuring people's security and protection from harm is typically the domain of governments and it may be appropriate and advantageous for governments to intervene in some of these areas where market forces do not appear to have brought about adequate levels of protection from malicious actors for internet users (Charney, 2002). As Mueller (2010) puts it, "Security more often than not is associated with efforts to reassert hierarchy and control. If anything can reanimate the desire for the nation-state, for traditional government, surely it is the demand for security." Framing internet governance issues as security matters is therefore strategically useful for government actors seeking to assert greater control over multistakeholder governance processes.

But while most stakeholders might be willing to concede the role of governments in ensuring security in the abstract, government stakeholder notions of security often clash with those of other stakeholders involved in the internet governance process. Perhaps nowhere was this tension more apparent than in the months leading up to WCIT, when the Arab states regional group submitted a proposal to amend the ITRs to include an article stating that "A Member State shall have the right to know through where its traffic has been routed, and should have the right to impose any routing regulations in this regard, for purposes of security and countering fraud" (Llansó, 2012). The proposal reportedly stemmed from concerns on the part of Arab states that their online traffic might be routed through Israel, thereby facilitating espionage efforts (Mueller, 2012). It was a proposal driven, in other words, by concerns about national security and protecting nation states' communications from interception by their foreign enemies. In the context of the Arab states' proposal on routing, however, government stakeholders' emphasis on national security priorities clashed with technical design features of the internet that were considered critical by technical and network operator stakeholders. Specifically, the requirement to inform nations of where their internet traffic was being routed and restrict routing paths would have required significant alterations of the existing internet infrastructure.

The proposal was criticised for its technical ramifications, with non-government stakeholders expressing concern that: "If the Arab States proposal were applied to all Internet communications, the requirement that countries be able to 'know' how every IP packet is routed to its destination would necessitate extensive network engineering changes, not only creating huge new costs, but also threatening the performance benefits and network efficiency of the current system" (Llansó, 2012). The government and industry stakeholders' views on security came into conflict here precisely because fulfilling the Arab states' vision of a secure internet, in which they could control the countries their packets flowed through, would have required implementing exactly the kind of network behaviour that technicians and operators would deem unexpected and insecure, in which packets respected national borders rather than being routed according to the most efficient or least congested pathways. Additionally, of course, the proposal

would likely have been hugely expensive and time-consuming for industry operators to implement.

While industry stakeholders pushed back against the proposal to give governments greater control over routing paths, civil society stakeholders also objected to the proposal—also in the name of security, but on very different grounds. Arguing that providing governments with information about how IP packets were routed might also serve to help countries keep track of what their citizens were doing online and who they were communicating with, privacy and security activists made the case that such practices could also be detrimental to individuals' online security. By allowing governments to block certain IP addresses or types of traffic, civil society stakeholders argued, "These types of regulations, which could be legitimized if the Arab States proposal is adopted, could threaten user rights to privacy and freedom of expression on the Internet" (Llansó, 2012). The proposal was ultimately not included in the revised version of the ITRs assembled at the 2012 WCIT, in part because of the considerable lobbying by technical industry stakeholders which successfully persuaded several national governments that such a proposal would be more detrimental to security than it would be helpful.

SECTION 5: ICANN AND DOTLESS DOMAINS

While industry and civil society were largely aligned in their perspectives on the security of the WCIT routing proposal, Google's 2013 proposal to purchase a "dotless" domain from ICANN gave rise to a conflict between competing views of security—and also competing views about industry competition—between private industry and civil society. In a letter to ICANN (Falvey, 2013), Google requested that it be permitted to operate the .search top-level domain as a dotless domain so that users who did not type in a fully-qualified domain name would be automatically directed to the .search domain, even if they did not explicitly type the full domain name. In their request, the company wrote: "Google intends to operate a redirect service on the 'dotless' .search domain (http://search/) that, combined with a simple technical standard will allow a consistent query interface across firms that provide search functionality, and will enable users to easily conduct searches with firms that provide the search functionality that they designate as their preference" (Falvey, 2013). This proposal, likely driven by business and economic factors, was quickly recast as an issue of security and stability by technical stakeholders involved in ICANN and internet governance. In Google's request, the idea is framed not as an effort to assert Google's dominance in the online search market (in fact, the letter explicitly states that users will be able to select their search function of preference and not be forced to use Google's), but rather as a matter of providing users with a "consistent query interface"—an interface that will behave as expected (or, securely) across a variety of different search firms.

The Internet Architecture Board (IAB), a body composed of technical experts, weighed in on the matter with a statement warning against issuing such domains due to concerns about security and stability. The IAB (2013) wrote:

> Since dotless domains will not behave consistently across various locations (and applications and platforms that may have different search list configuration mechanisms), they have the potential to confuse users and erode the stability of the global DNS. By attempting to change expected behavior, dotless domains introduce potential security vulnerabilities. These include causing traffic intended for local services to be directed onto the global Internet (and vice-versa), which can enable a

> number of attacks, including theft of credentials and cookies, cross-site scripting attacks, etc.

This notion of security adheres closely to the technical definition of a secure computer system as one that behaves as expected. The IAB was not concerned about the national security or social implications of dotless domains (at least, not directly) but rather about the potential for these domains to "change expected behavior". The ICANN Security and Stability Advisory Committee (SSAC), another body representing neither industry nor governments, also issued a report (2012) advising against issuing dotless domains as they could lead to unexpected, and potentially malicious, outcomes (Zusman et al., 2013).

Following these recommendations, at an August 2013 meeting, ICANN adopted a resolution prohibiting dotless domains. Notably, the civil society stakeholders who were most vocal about their security concerns related to implementation of dotless domains enjoyed considerable support from government stakeholders and even some industry stakeholders—especially those who viewed Google as a competitor—in this debate. The ICANN Governmental Advisory Committee (GAC) also voiced objections to Google's proposal and supported the position taken by the IAB and SSAC. The GAC's willingness to go along with the civil society stakeholders' recommendations on this matter suggests that there are, in fact, concrete points of agreement among the internet governance community around what types of security are desirable, especially from a technical standpoint. It also speaks to the fact that more than competing versions of security, this case seemed to exhibit an underlying tension between market competition and security. Often, however, it is harder for stakeholders to reach consensus when dealing with the notions of security that derive not from the technical world, but from the government and civil society stakeholder groups.

SECTION 6: WHOIS DATABASE POLICIES

Arguments about security were also at the heart of the controversy over a 2015 proposal to ICANN to alter the privacy policy governing the WHOIS database, which contains information on the people and organisations who own and operate domain names. The 2015 proposal would limit access to privacy and proxy services that conceal domain owners' personal information in the publicly accessible WHOIS database. Under the proposal, the owners of any website that includes commercial or transactional services of any kind (including donations, sales, etc.) would be required to keep their contact information, including name, address, phone number, and email, publicly available in WHOIS. The proposal led to a clash between government and civil society representatives in the multistakeholder process, with both supporters and critics of the controversial proposal couching their reasoning in terms of security concerns.

Supporters of the WHOIS proposal included the GAC Public Safety Working Group (PSWG), which stated in a report (2016) that: "In order to promote transparency and consumer safety and trust, the PSWG recommends against permitting websites actively engaged in commercial transactions—meaning the collection of money for a good or service—to hide their identities using Privacy/Proxy (P/P) Services." The government stakeholders in the GAC and PSWG viewed the disclosure of personal information about people undertaking online commercial transactions as a matter of national security and safety. "The public is entitled to know the true identity of those with whom they are doing business," they wrote, emphasising the need for public safety authorities and law enforcement officers to be able to identify and track down

individuals from their online activity. “To the extent privacy services are used to hide the actors responsible for malicious activities or obscure other pertinent information, there must be reasonable mechanisms in place for public safety authorities to unmask bad actors and obtain necessary information,” the GAC PSWG concluded (2016), affirming their national security perspective on the issue.

Civil society stakeholders, meanwhile, offered a different assessment of the proposal to limit privacy and proxy services for WHOIS focused on individual security rather than national security and public safety. Among privacy and security advocates, the proposal was widely criticised for making it more difficult for online users to avoid harassment. Jeong and Albert (2015) argue, "For many, particularly those who become the targets of online harassment, WHOIS proxy or privacy protections are vital for their safety". At issue here are two very different conceptions of who is being secured from what: are the innocent online fundraisers and entrepreneurs being protected from harassers and political retribution, or are innocent internet users being protected from online crooks and website scams? Government representatives were hewing to notions of national security and public safety that emphasised the latter, while civil society representatives were embracing a notion of individual or human security that highlighted the former.

CONCLUSION

The tensions that arise around issues of security among different groups of internet governance stakeholders speak to the many tangled notions of what online security is and whom it is meant to protect that are espoused by the participants in multistakeholder governance forums. What makes these debates significant and unique in the context of internet governance is not that the different stakeholders often disagree (indeed, that is a common occurrence), but rather that they disagree while all using the same vocabulary of security to support their respective stances. Government stakeholders advocate for limitations on WHOIS privacy/proxy services in order to aid law enforcement and protect their citizens from crime and fraud. Civil society stakeholders advocate against those limitations in order to aid activists and minorities and protect those online users from harassment. Both sides would claim that their position promotes a more secure internet and a more secure society—and in a sense, both would be right, except that each promotes a differently secure internet and society, protecting different classes of people and behaviour from different threats.

While vague notions of security may be sufficiently universally accepted as to appear in official documents and treaties, the specific details of individual decisions—such as the implementation of dotless domains, changes to the WHOIS database privacy policy, and proposals to grant government greater authority over how their internet traffic is routed—require stakeholders to disentangle the many different ideas embedded in that language. For the idea of security to truly foster cooperation and collaboration as a boundary object in internet governance circles, the participating stakeholders will have to more concretely agree on what their vision of a secure internet is and how it will balance the different ideas of security espoused by different groups. Alternatively, internet governance stakeholders may find it more useful to limit their discussions on security, as a whole, and try to force their discussions to focus on more specific threats and issues within that space as a means of preventing themselves from succumbing to a façade of agreement without grappling with the sources of disagreement that linger just below the surface.

The intersection of multistakeholder internet governance and definitional issues of security is

striking because of the way that the multistakeholder model both reinforces and takes advantage of the ambiguity surrounding the idea of security explored in the security studies literature. That ambiguity is a crucial component of maintaining a functional multistakeholder model of governance because it lends itself well to high-level agreements and discussions, contributing to the sense of consensus building across stakeholders. At the same time, gathering those different stakeholders together to decide specific issues related to the internet and its infrastructure brings to a fore the vast variety of definitions of security they employ and forces them to engage in security-versus-security fights, with each trying to promote their own particular notion of security. Security has long been a contested concept, but rarely do these contestations play out as directly and dramatically as in the multistakeholder arena of internet governance, where all parties are able to face off on what really constitutes security in a digital world.

REFERENCES

GAC Public Safety Working Group Comments to Initial Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process. (2016, March 9). Available from https://gacweb.icann.org/display/GACADV/2016-03-09+Privacy+and+Proxy+Services+Accreditation+Issues?preview=/41943982/41943981/ANNEX%20A%20-%20PSWG%2BGAC%20comments%20proxy%20privacy%20accreditation%20issues.pdf

Proposals for the Work of the Conference. (2012, December 3-14). Submitted by Russia, UAE, China, Saudi Arabia, Algeria, Sudan, and Egypt, World Conference on International Telecommunications (WCIT-12). Available from Available from http://files.wcitleaks.org/public/Merged%20UAE%20081212.pdf

Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies* vol. 23, no. 1, pp. 5-26.

Beautement, A., & Pym, D. (2010). Structured systems economics for security management. In *Proceedings of the Ninth Workshop on the Economics of Information Security*. Cambridge, MA, USA.

Cavelty, M. D. (2010). Cyber-Security. In *The Routledge Handbook of New Security Studies*. (Peter Burgess ed.) London: Routledge, pp. 154-162.

Charney, S. (2002). Transition Between Law Enforcement and National Defense. In *Security in the Information Age: New Challenges, New Strategies*. (Robert F. Bennet ed.), available from http://www.iwar.org.uk/cip/resources/senate-2002/security.pdf

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Epstein, D., Ross, M., and Baumer, E. (2014). It's the definition, stupid! Framing of online privacy in the Internet Governance Forum debates. *Journal of Information Policy*, vol. 4, pp. 144-172.

Falvey, S. (2013, April 6). "Re: Update on Amendments to Four of Charleston Road Registry's Applications." Letter of Christine Willett, General Manager, ICANN gTLD program. Available from http://assets.sbnation.com/assets/2455295/falvey-to-willett-06apr13-en.pdf

Garfinkel, S. and Spafford, G. (2003). *Practical UNIX and Internet security*. O'Reilly Media, Inc.

ICANN Security and Stability Advisory Committee. (2012, February 23). SSAC Report on Dotless Domains. Available from https://www.icann.org/en/groups/ssac/documents/sac-053-en.pdf

"International Telecommunication Regulations." (2012). Final Acts: World Conference on International Telecommunications, Dubai. Available from http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

Internet Architecture Board. (2013, July 10). IAB Statement: Dotless Domains Considered Harmful. Available from https://www.iab.org/documents/correspondence-reports-documents/2013-2/iab-statement-dotless-domains-considered-harmful/

Jeong, S. and Albert, K.. (2015, July 2). An Unassuming Web Proposal Would Make Harassment Easier. *Wired*. Available from http://www.wired.com/2015/07/unassuming-web-proposal-make-harassment-easier/

Llansó, E. (2012, Sept. 6). Security Proposals to the ITU Could Create More Problems Not Solutions. Center for Democracy and Technology. Available from https://citizenlab.org/cybernorms2012/CDT2012.pdf

Mueller, M. L. (2010). *Networks and states: The global politics of Internet governance*. MIT Press.

Mueller, M. L. (2012, June 21). Threat Analysis of the WCIT Part 4: The ITU and Cybersecurity. Internet Governance Project. Available from http://www.internetgovernance.org/2012/06/21/threat-analysis-of-the-wcit-4-cybersecurity/

Parker, D. B. (1998). *Fighting Computer Crime: A New Framework for Protecting Information*. Wiley.

Rothschild, E. (1995) What is security? *Daedalus*, Vol. 124, No. 3, pp. 53-98.

Ullman, R. H. (1983). Redefining Security. *International Security*, Vol. 8., No. 1, pp. 129-153.

Wolfers, A. (1952). "National Security" as an Ambiguous Symbol. *Political Science Quarterly* vol. 67, No. 4, pp. 481-502.

Zusman, M., J. Allen, and R. Umadas. (2013, July 29). Dotless Domain Name Security and Stability Study. Available from https://www.icann.org/en/groups/ssac/documents/dotless-domain-study-29jul13-en.pdf

Declaration of novelty and no competing interests:

By submitting this manuscript I declare that this manuscript and its essential content has not been published elsewhere or that it is considered for publication in another outlet.

No competing interests exist that have influenced or can be perceived to have influenced the text.