Bridges: Conversations in Global Politics and Public Policy

Virtual Roadblocks: The Securitisation of the Information Superhighway

A. T. Kingsmith, York University

Bridges: Conversations in Politics and Public Policy (2013) 1(1)

Abstract

The Internet we know today is both content filtered and packet shaped. Subsequently, it is not the free operating zone of meta-space early proponents expected. Contrary to conventional wisdom, a multitude of actors have shown an increased willingness to intervene and control communication via the Internet with precision and effectiveness. This paper employs the Copenhagen School's conceptualisation of securitisation at the macro level to address the issue of global Internet filtering from a "network" position between traditional "national" security and critical "individual" security. It looks at the ways in which intervention into the Internet's infrastructure is leveraged for governance through various research programs such as Ronald Deibert's Open Net Initiative, which probes all aspects of a national information infrastructure over the long term, concluding that the scope, scale, and sophistication of global Internet filtering are increasing in non-transparent fashions.

It should come as no surprise that since its dissemination, authoritarian regimes such as China, Iran and, Saudi Arabia have actively engaged in Internet filtering practices. What is troublesome is that advanced industrialised countries including Canada, Germany, and the United States have also followed suit. Reasons for doing so include: the securitisation of information communication after 9/11, to restricting access to material involving the sexual exploitation of children as well as 'extremist' websites. Considering these securitising moves, this paper argues that the more that filtering practices are withheld from public scrutiny and accountability, the more temping it is for framing authorities to employ these tools for illegitimate reasons such as the stifling of both opposition and civil society networks. Furthermore, due to increased connectivity, transparent Internet requires desecuritisation of social agents and international security structures in order to ensure more free information.

Keywords: Copenhagen School, securitisation theory, Internet, desecuritisation, hypermedia, macrosecuritisation

To cite this Article: Kingsmith, A T. (2013) "Virtual Roadblocks: The Securitisation of the Information Superhighway," *Bridges: Conversations in Global Politics and Public Policy*: Vol. 2: Iss. 1, Article 3.

Introduction

In 2007, Bill Gates proudly proclaimed that the Internet was becoming something of a town square for the global village of tomorrow. We might find Gates' optimism reasonable, even warranted considering the ideas, messages, news, information, and money that reverberate around the world in seconds, crossing borders and time zones instantaneously, characterising an age of free and readily available information – an age where charities, banks, corporations, governments, nongovernmental organisations, and radical establishments alike all use the Internet to do business, organise, and communicate. In its relatively short lifespan, the Internet has evolved from a laboratory research tool into a globally immersive environment of cyberspace that encompasses the entire connected world. However, this transition towards inter-connectedness has not been a seamless one. Since the Internet provides many groups with alternative modes of organising critical social interactions, institutionalising political movements, and advancing economic demands, it also generates new challenges concerning how to create, border, police, govern, and use virtual spaces (Swiss 2000).

In addition to these challenges, states – and at times industries acting under state mandate – have shown an increased competence, exactitude, and willingness to intervene in an attempt to control communication over the Internet. For as much as Internet accessibility is dependent upon the simple willingness of governments to allow their citizenries unmitigated access to the Web, critical analyses of state cyberspace policies reveal disconcertingly institutionalised regimes of panoptic surveillance. While it is true that Internet relations in the digital environment are embedded within complex networks, a common societal misconception persists that technical imperatives cause states to operate according to the physical boundaries of cyberspace. However, most of these "technical" decisions are made on purely aesthetic, commercial, financial, social, cultural, or political grounds, as opposed to legitimate engineering criteria. Thus, the aesthetic prejudices, commercial aspirations, financial targets, social fears, cultural semblances, and political ontologies of the hardware designers, software vendors, and network providers shape the domain of permissible digital behaviours. Far from being innately emancipatory in nature, cyberspace can be used to reinforce hegemonic powers, cultivate a culture of fear, and avert or minimise political opposition (Warf 2010).

Society is in the early stages of the struggle for digital freedom. The future of free and open Internet is therefore largely dependent on what happens in the next few years. In order to understand these unfolding challenges, this paper will employ the critical security approach of the Copenhagen School's securitisation theory at the macro – supranational level to examine the global practice of Internet censorship. It will do this by laying the theoretical foundations of macrosecuritisation and then applying them, both theoretically and practically, to the securitisation of cyberspace. It will then compare and contrast cyber-utopian and hyper-securitised conceptualisations of the Internet in order to disclose the rationales behind – and extensiveness of, the securitisation of the Internet network. In addition, this paper will explain the practices of "content filtering" and "packet shaping" shared by a multitude of actors to censor Internet traffic – concluding with a theoretical and practical discussion of how to desecuritise the Internet by re-subjecting it to democratically normalised political discourse. "Virtual Roadblocks" will employ these methods in order to argue that the Internet must be macro-desecuritised. The more filtering practices are withheld from public scrutiny and accountability, the more temping it is for framing authorities to employ censorship tools for illegitimate and arbitrary reasons such as the stifling of oppositions or civil society networks. The myth of ungovernability derives from illusions regarding the decentralised architecture of the Internet. Securitisation theory can shatter this myth and expose the extent to which the Information Superhighway is governed.

Framing the Discourse: The Copenhagen School's Securitisation Theory

The various ways in which the Internet can be said to threaten security is context-dependent. According to Didier Bigo (2002), security can refer to human, state, or sub-state threats – effectively resulting in a convergence between the meanings of international and internal security. However, threats to one may not entail threats to others. Since cyberspace is characterised by rapid cross-border communication, analyses of Internet security must employ a critical perspective unrestrained by the geographies and the discourses of state power. Such a perspective can be found within the Copenhagen School, comprised mainly of the collective works of Ole Wæver et al. (1993) and Barry Buzan et al. (1998) – both of whom have published collections pertaining to regional security complex theory and the interrelationships between regions and global security (Peoples and Vaughan-Williams 2010). While occasionally portrayed as distinctively European contributions to debates over the social construction of security, the Copenhagen School's concepts have developed a broad and powerful research agenda across the field of International Security Studies – being employed, critiqued, and expanded through debates initiated far beyond the geographical or intellectual confines implied by the notion of a "school" (Peoples and Vaughan-Williams 2010).

These debates, which contest the nature and meaning of "security," have become the focus of renewed controversy in security studies. According to Michael C. Williams (2003), the Copenhagen School considers questions surrounding the broadening of the security agenda to include threats beyond the conventional rubric of state and military security, embracing the claim that this agenda must also be deepened to include the security concerns of actors ranging from individuals and sub-state groups – articulated as human security, to global concerns such as the environment, which have often been marginalised within traditional state and militarily-centric conceptualisations. As references to "possible or actual threats" are problematically linked to impossibly "objective" definitions of security, the Copenhagen School argues that to study the social construction of security, it must be seen in both the context of shifting agendas, and as part of the broader theoretical movement (Williams 2003). The broadening of the security agenda and the debunking of positivistic ambiguities can be achieved by employing a discursive conceptualisation of security developed by Wæver (1993) referred to as the "securitisation" approach, which makes security entirely dependent on its successful construction within discourse.

In securitisation theory, security is treated not as an objective condition but as the outcome of a specific social process. The social construction of security issues – who or what is being secured, and from what – is analysed by examining "securitising speech-acts," actions or statements through which existential threats become represented and recognised (Williams 2003). Yet the actual word "security" is not necessary for the specific nature of the speech-act – though it often plays a vital role, but the broader rhetorical performance, which far from being limited to linguistics, increasingly includes visual and graphic imageries. This stance allows the Copenhagen School to argue simultaneously for both an expansion and a limitation of the security agenda and its analyses. On the one hand, treating security as a speech-act allows for an almost indefinite expansion of the security agenda. Not only are the realms of possible threats enlarged, but also the actors or objects that are threatened – termed "referent objects" of security – can be extended to include actors and objects well beyond the military security of the territorial state (Williams 2003). Conversely, while treating security as a speech-act allows a remarkable broadening of analyses, securitisation theory also seeks to limit the security agenda. As Buzan (1998) notes, security is not synonymous with harm or with the avoidance of whatever else might be deemed malign or damaging. As a speech-act, securitisation then has a specific structure, which in practice limits the theoretically unlimited nature of security.

This leads to the question of how a successful speech-act takes place. According to Wæver (1995), an actor engages language of exceptionalism – such as "security, "risk," "terror," or "danger," in order to frame an event as extraordinary, thereby justifying the use of whatever means necessary to prevent said event. In other words, a person or event becomes securitised and thus treated in the same degree of urgency as a military threat (Peoples and Vaughan-Williams 2010). Think of a government realising a statement or address (speech act), justifying increased security on the Web (referent object), in order to deter terrorism, or cybercrimes (existential threat). Buzan and Lene Hansen (2009) note that we can think of this process of securitisation in terms of a spectrum that runs from non-politicised through politicised to securitised – the issue is an existential threat that justifies responses that go beyond normal policy practices. Case in point, "emergency" acts such as the American PATRIOT Act, or Canadian Anti-Cybercrime Bill C-30. Vulnerabilities have to be staged as existential threats to a referent object by a securitising actor, who "thereby generates endorsement of emergency measures beyond rules that would otherwise bind" (Buzan 1998: 5). However, according to Williams (2003: 514), claims that are likely to be effective, objects to which they refer, and social positions from which they can effectively be spoken are "usually deeply sedimented – rhetorically, discursively, culturally, and institutionally – and structured in ways that make securitisations somewhat predictable and thus subject to probabilistic analysis."

Expanding the Discourse: Desecuritisation, Macrosecuritisation and the Network

In contrast to traditional assumptions that security is an intrinsic good, the most striking supposition of securitisation theory is that security is not always positive. Since security can create polarising false dichotomies – threat or decision, friend or enemy – it is something to be invoked with great care and minimised rather than expanded. In most cases Wæver (1995) argues that we should strive for desecuritisation, or the shifting of issues out of emergency mode into the normal bargaining processes of the political sphere. If successful, desecuritising moves can replace the problematic conditions of security with the optimal conditions of "asecurity," where actors "who do not feel insecure, do not self-consciously feel or work on being secure – [for] they are more likely to be engaged in other matters" (Wæver 1998: 71). While this still leaves the question of how issues that have already been successfully securitised might be downgraded back to "normal" status, the majority of critical security scholars agree that solutions to securitising moves are case specific, and that uniform approaches to desecuritisation devoid of context and critique are inherently problematic and unsuccessful.

In principle any actor can make a securitising move. In practice however, the majority of securitising actors are political leaders, bureaucracies, states, intergovernmental organisations, and lobby groups (Buzan and Hansen 2009). Working within their distinctive approach to securitisation, the Copenhagen School has begun to expand traditional conceptions of securitisation beyond referent objects at the state-level to include "macrosecuritisations," multiparty security arrangements between multiple states and organizations which "aim at structuring international politics on a larger scale" (Buzan and Hansen 2009: 214). While macrosecuritisations are subject to the same rules that apply to other securitisations, they operate transnationally, packaging together securitisations from various levels beyond borders into a "higher and larger" order (Buzan and Wæver 2009). With the advent of the Internet age, macrosecuritising collaborations are emerging with increasing frequency due to improved means of communication – an example would be the all-encompassing "War on Terror," which amalgamates over 100 national security policies into an international anti-terrorist cooperative. Such a regime adds an enlarged dimension to the relationship between the securitising actors by bringing into play a variety of possible multilateral partnerships, which generate "social structures and rhetorical resources capable of overcoming the normal parochialism that favours securitisations at the middle, unit-to-unit, level" (Buzan and Wæver 2009: 275).

According to J.P. Singh (2010), even a macrosecuritisation such as the War on Terror, understood within the multiplicity of speech acts, and the referent objects of military, political, societal, environmental or human, only takes the world "as-was," not how it has been transformed by technology. Hence macrosecuritisations are becoming increasingly more aware of the Internet's enabling of new, nimble, and distributed challenges to public and private institutions worldwide – manifested in mobilised opposition movements, protests, and in extreme cases, revolutionary change. The referent object to be securitised is no longer a singular security form such as terrorism. Rather, the object to be secured is a borderless world of free-flowing information, a single seamless environment where ideas can be shared fluidly within a cyberspace that is not controlled by spatial and temporal conceptualisations of security. Unsurprisingly, the motivations for securitising such a network range widely from concerns over national security, cultural sensitivity, and protection of social values, to rent seeking and the protection of economic monopolies. A quick look at the recoil from the actions of individuals and organizations such as Edward Snowden, Bradley Manning, and WikiLeaks show the swiftness and ruthlessness in which governments respond to anything or anyone they perceive to be a possible threat to digital macrosecuritisations. For as Ron Deibert (2012) points out, even states of conflicting economic and political orientation are collaborating to limit and control the Internet. And due to the constitutive nature of the collective images of security, these collaborations are becoming more and more successful at macrosecuritising cyberspace.

Shutting Down the Discourse: The Securitising of Hypermedia

Hypermedia is a term employed by contemporary media theorists to denote a world deeply saturated with "new technologies of digital-electronic telecommunications…that are transforming economics, society, and politics" (Potter 2002: 27). In one formulation we are told that we experience a hypermedia network spurring an information revolution that is breaking down hierarchies, authoritarian regimes, and closed societies while generating openness, integration, freedom, and democratic tranquility. In the other, we are warned that the panoptic power of states and corporations allows these bodies, with the aid of cyber-spatial tools of surveillance, to penetrate the private lives of individuals (Gandy 1993). While such work has clearly demonstrated that the Internet can be made to work against people as well as for them, both of these hyper-libertarian and the hyper-fascist conceptualisations of hypermedia are mutually exclusive, and rely upon a false dichotomy which makes simplistic and deterministic suppositions that new technologies perpetuate either freedom or control. As Deibert (1997) notes, such assumptions overlook the fact that digital technologies are never inherently "of anything" apart from the social context in which they are situated. To say that hypermedia negates technology of either freedom or oppression ignores the contextual nature of both securitisation and desecuritisation. It never asks the questions, "freedom from what or whom?" and "control over what or whom?"

In the normative sense, broad and informal Internet filtering of a free, public, and unitary digital network is an infringement of civil liberties and human rights. However, many states insist they have the right to control internal matters – whether or not they occur in cyberspace, and that there is often little that other states, institutions, or lobbyists can do to convince them otherwise. As mentioned previously, governments advocate securitising the network for a plethora of reasons such as protecting public morality from ostensible sins such as pornography or gambling – although more recently combating terrorism has emerged as a favorite rationale. Deliberately vague notions of national security and social stability are typically invoked, which hold that some degree of censorship is needed to combat "cyberanarchy" or to prevent cybercrime (Goldsmith 1998). Yet the state is no longer simply an internal meta-entity that can securitise social, economic, and political referent objects solely within its territory. Today governments are amalgamated through regulatory institutions, market forces, and information flows that comprise of multiple layers of authority. Thus erosion between politics within and beyond states has caused boundaries to become blurred and fragmented to such a degree that even inherently domestic policy prescriptions may to have overarching consequences for many other members of the international community.

Moreover, digital expression is increasingly controlled, facilitated, and regulated by a small handful of powerful conduits working under governmental supervision. According to Dawn Nunziato (2009), the regulation of cyberspace has evolved so as to grant these private entitles – search engines, broadband/backbone providers, and email providers – unfettered agency regarding censorship practices. These securitising moves are resulting in the emergence of an increasingly Balkanised Internet, meaning the cyber-utopian ideal of the network as a desecuritised and unregulated digital libertarianism no longer holds much currency. The current reality of the Internet is one of control being continually and forcefully reasserted online. Theorists who cling to this digital libertarianism may continue to suggest that the Internet encapsulates an alternative jurisdiction that is almost impossible to regulate, that the network is still free of state influence, and this, coupled with its unprecedented ease of entry, allows the Internet to serve as a monumental forum for free expression. Yet such an idealistic view of a desecuritised World Wide Web as a Radio Free Europe on steroids is what Evgeny Morozov (2011) refers to as "net delusion," an overly idealistic view of the Internet as an inherently emancipatory and unregulated tool. A view that ironically enough, actually serves to further securitise the Web by lulling users and activists into a false sense of online confidentiality.

How It's Done: The Mechanics of Securitisation

As the previous analyses have illustrated, the Internet is not an uncontrolled ethereal virtual space. Rather, it is a real physical network of networks that has become an object of geopolitical contestation. Instead of a World Wide Web, Jonathan Zittrian and John Palfrey (2008) contend that it is more accurate to say that we have a Saudi Wide Web, an Uzbek Wide Web, a Pakistani Wide Web, a Thai Wide Web, and so forth. What they mean by these sentiments is that the network is very much a governed space. According to Deibert and Rafal Rohozinski (2010) such securitised governance occurs in at least three ways. First, by the rules of physics as well as code, which give the Web predictable and finite characteristics. Second, by normative consensus amongst Internet service providers and operators, without whom the network could not function. Third, by governance of actors – states, corporations, and civic networks, which understand how leveraging and exploiting key nodes within the physical structure of the Internet can give them strategic political, social, and economic advantages. Each of these nodes presents an opportunity for various authorities to impose order on Internet traffic through some mechanism of filtering and surveillance with which to seek out sources of information framed as strategically threatening.

While some of this control takes place for reasons of efficacy, the majority of network macrosecuritisation is under the auspices of more subjective political, cultural, or social securitising moves. These actors deliberately shroud their governance in an informal secrecy, and indeed benefit from the promulgation of the myths of cyber-utopianism and asecurity communities in order to shield their activities from public discourse (Deibert and Rohozinski 2010). The myth of ungovernability derives from illusions regarding the decentralised architecture that characterises the Internet. The World Wide Web is not a pure network. It is both distributional and hierarchical, making some nodes of connectivity more important than others. Key nodes in the Internet infrastructure provide critical chokepoints where filtering and surveillance mechanisms can be imposed (Wilson 2009). The ten "Tier 1" telecommunications providers – of which seven are in the U.S., and therefore subject to American law, connect to the entire Internet while other tiers only connect to portions of it, meaning that the entire digital framework rests on a system of highly regulated global transit networks at 150 Internet exchange points (Deibert and Rohozinski 2010).

Although it may be rare for electronic surveillance to enter the public discourse, to varying degrees states employ a mechanism of "best practices" in order to synthesise a set of "network interrogation techniques to intercept and monitor communications traffic at key Internet chokepoints within and beyond their territorial boundaries" (Deibert and Rohozinski 2010: 260). These best practices are methods on how to control the rate of traffic received on a network interface – rate limiting, the most widespread of which are "content filtering" and "packet shaping." Content filtering – done by inserting software that reroutes data along the Internet's pathways, is the practice of restricting access to information by selectively blocking user requests for data from being completed (Zittrian and Palfrey 2008). Packet shaping – or traffic shaping, employs a complex algorithm that slows the rate of data transfer to a point where the user's desired page will be unable to load (Blake 1998). These methods to filter Internet content are becoming progressively more sophisticated, and securitising authorities are becoming increasingly more proficient at employing rate limiting to target newly inundated modes of information dissemination, such as blogs, social media sites, and mobile messaging.

The above first-generation filtering practices rely on passive means, in which lists of banned websites are loaded into routers so that requests to servers hosting those websites are denied. According to communiqués from the hacker community, these methods – employed by countries such as China, Iran, and Saudi Arabia, are relatively unsophisticated and easy to bypass and detect (Pariser 2011). It is therefore not surprising that first-generation methods are being supplanted by next-generation strategies intended to be more stealthy, dynamic, and sophisticated. According to Deibert and Rohozinski (2010), these streamlined filtering practices are more effective because they are self-aware that the value of information is not fixed in time. Therefore, filtering is only initiated when information has the greatest value – such as an election season. Next-generation strategies also specifically target critical resources, as opposed to broad-brush censorship of whole categories of content, and adapt to technological limits of less developed states, for example, there is evidence that next-gen methods were employed by Ethiopia, Uganda, and Cambodia to shut down SMS services during 2007's political anxieties.

Down the Rabbit Hole: How Securitised is the Network?

The early theorising about Internet regulation centred on the extent to which states could and would regulate the activities of individuals in cyberspace. However, as the malicious strategies employed to securitise the network have shown, this kind of state-to-individual regulation is a given today. According to Deibert (2012), securitisation now involves a fusion of regulation in which states take a leadership role in best practice sharing alongside a multitude of other actors with a stake in cyberspace policies and practices. The majority of non-state actors are large private corporations who manufacture filtering software used to block content. Internet security companies, such as *Fortinet*, *Secure Computing*, and *Websense*, create off-the-shelf filtering products that block access to categorised lists of websites. While these products are primarily marketed to businesses, they have been readily employed by censoring states such as Tunisia (*Secure Computing*), Iran (*Secure Computing*), Myanmar (*Fortinet*), and Yemen (*Websense*), to block access to politically sensitive content (Deibert 2008). These governments simply tick off categories of websites they do not want accessed, such as "advocacy groups" or "militancy and extremist groups," the most securitised categories in *Websense*'s database.

The technological, economic, and social shifts caused by network securitisation continue to be driven by the changes in the ways governments assert themselves in cyberspace. Macrosecuritisation strategies are now spreading virally, from regime to regime, as legitimate means to assert state power and control in order to disable adversaries. The visibility and relative maliciousness of precise assertions of state power vary depending on the regime, but a multitude of states are participating in a considerable and overt macro-organisation of securitisation that is driven by the omnipresent desire – regardless of political orientation – to minimise dissent and opposition, promote and protect national identity and territorial control, and respond to selectively and subjectively framed domestic "terrorist threats." According to Deibert (2012), the majority of the norms driving network controls emanate from policies initiated by liberal-democratic and advanced-industrialised countries. Within Western regimes, governments and corporations – under government instruction, are developing wide-ranging and ambitious interventionist strategies in cyberspace, from the setting up of units within their armed forces dedicated to "fighting wars" in cyberspace, to introducing legislation on surveillance, data retention, and best practice sharing with friendly and not-so-friendly regimes.

From democratic to autocratic, governments are developing and sharing wide-ranging and ambitious interventionist strategies in cyberspace. What securitises the network is not these middle-level securitisations such as China's "Great Firewall," the United States' "PATRIOT Act," or Saudi Arabia's "Culture Controls," but how they amalgamate together with private corporations at the state level and beyond to securitise the macro. Increasingly, these amalgamations where best practices are shared and policies coordinated are among regional security organisations. Recently, the Shanghai Cooperative Organisation (SCO), the Gulf Corporation Council (GCC), and the North Atlantic Treaty Organisation (NATO), have begun to deal with cyberspace issues in a concerted fashion. According to Deibert (2012), in 2010 NATO affirmed a greater commitment to joint cyberspace operations and doctrine, in 2009 the SCO coordinated practices and joint exercises around "information security" and "cyberwar" to counter mass social mobilisation, and since 1997 the GCC has adhered to similar policies regarding "traditional practices and religious beliefs" of growing Internet connectivity. These sharing practices – and others such as the agreement between the spy agencies of Canada, the United States, Australia, New Zealand and the United Kingdom codenamed the "Five Eyes" – are connecting many states across political, social and securitised spheres in a high-level macrosecuritising organisation that seeks to keep the network restricted in order to maintain a status quo that heavily monitors and restricts the potential for organised collective dissent.

The Theoretical: Desecuritising the Macrosecuritisation 1.0

Since the production of insecurity and the designation of issues and actors as threats to society are part and parcel of the re-iterative, performative production of state identity (Campbell 1998), network securitisation at the macro level is not all that surprising. States continuously securitise issues and actors in order to construct a national identity, "rallying around the flag." Consequently, desecuritisation is perhaps best understood as the fading away of one particular issue or actor from the repertoire of these processes. At some point, certain "threats" might no longer exercise our minds and imaginations sufficiently, and as such, they must be replaced with more powerful and stirring imageries. Yet to declare that a particular issue or actor no longer constitutes a security threat and does not require extraordinary measures simply opens up a "language game," in which more often than not the correctness of the declaration, its implications, and its consequences, become the topic of further debate (Behnke 2006). Hence, the issue or actor never leaves the discourse of security within which the securitisation embedded it. Moreover, even a denial of a connection still maintains the potentiality of that connection, meaning that the Internet can only become desecuritised through the eradication of all securitising speech, and a return to the "normal' language of the strictly political.

If we agree with Wæver (1995) and stress the need for desecuritisation, then the question is how to unmake the fabrication of an open network as an existential threat to the securitising actors. This problem locks actors into talking merely in terms of security, reinforcing the hold of security on our thinking, even if our approach is a critical one. According to Jef Huysmans

(1998), a self-reflexive interpretation of security develops this perspective by exploring the political rationality within which securitising practices emerge. Self-reflexivity engages ethical and political questions regarding the organisation of the political that arise from the structuring work of security practices, particularly from framing free-speech and open information as existential threats. Thus, desecuritisation is only possible when we move the issue of a free and borderless world of information available to all off of the security agenda back into the realm of public discourse with normalised political debate and accommodation. Size and scale of form seem to be one crucial variable in determining what is or is not a successful referent object of security. At the micro end of the spectrum, individuals or small groups can seldom establish wider security legitimacy in their own right. They may speak security to, and of, themselves, but few others will listen. While some actions may at first seem to be about individual security, the referent object is often better understood as a universalistic principle at the system or subsystem level (Buzan and Wæver 2009).

The Practical: Desecuritising the Macrosecuritisation 2.0

Taking into account the extraordinary measures and exceptional politics that securitisation is steeped in, desecuritisation can be regarded as a political choice to restore the Internet's democratic principles. According to Claudia Aradau (2004), the question of desecuritisation is therefore about the kind of politics we want. Do we want the parsimonious politics of exceptional measure, or do we want the contested politics of democratic procedure? As desecuritisation is the democratic challenge to the non-democratic politics of securitisation, it has to be inscribed institutionally in order to create a different relation not rooted in the exclusionary logic of security. Desecuritising the network is about looking at the micro, the meso, and the macro, recognising larger scale institutional forms where a set of interlinked securitisations become a significant part of the social structure of international society. We need to confront the patterns of unaccountably and non-transparency of Internet practices by states and corporations that censor. While there is certainly a legitimate debate to be had about the balance between a state's right to cultural sovereignty and the free flow of information raised by Internet censorship, most states do not allow such a debate to take place prior to filtering, refusing to display transparency regarding content blocked and filtering practices employed – thereby evading the desecuritising shift into language of the everyday.

Accountability and transparency issues plague the disclosure of securitised filtering practices. Among states and non-state institutions that filter, few are willing to admit the full scope, scale, and precise nature of their filtering systems (Deibert 2008). Securitised actions which monitor, interfere, censor, restrict, and control on a level that is beyond public discourse are incompatible with democratic societies. We need a transparency that considers the presence of concealed filtering, provisions to appeal or report instances of inappropriate blocking, and open acknowledgement of filtering policies. The good news is that macrosecuritisations have a more complicated structure than ordinary ones. Because they contain both higher and lower level securitisations built upon multilateral collaboration, they embody permanent tensions across levels and are thus vulnerable to breakdowns not just by desecuritisation of the macro-level threat (referent object) but also by the middle and micro-level securitisations – such as a state or corporation, becoming disaffected with, or pulling away from, subordination to the higher level one (Buzan and Wæver 2009). The macro-desecuritisation of the network can be attempted by contestation at the lower levels through grassroots transnational social movements aimed at protecting and preserving the Internet network as an open commons of information. The movement must employ language of normal political discourse, work alongside organisations like WikiLeaks, provide support for data leakers such as Snowden and Manning, mobilise interest groups and major NGOs – such as Amnesty International and Reporters Without Borders, and direct at multiple levels, from the construction of censorship circumvention technologies and other "hacktivist" tools, to lobbying for the promotion of norms of openness and access to information at international and institutional levels.

We must be vigilant to prevent further securitisation, and drive desecuritisation by being both smart and vocal. To be smart means employing free and secure protection tools. Some of the more popular ones include "RiseUp" an email service that sends emails without the government monitoring your actions as the connection is encrypted; "Eraser," which allows journalists to securely and temporarily delete files that can be recovered later should their data be seized; "Tor Browser," a Mozilla Firefox-based browser that allows users a secure tunnel to the Internet and hides your digital online identity in case you're being monitored; "Cobian Backup," running in the background, the program allows users to quickly and effectively back up their data; and "Pidgin," an open-source instant messenger that allows users to connect to several instant messaging accounts and services. To be vocal means employing multiple avenues of expression in desecuritising through apolitical speech-acts that question past, present, and future attempts to move discussions regarding network security beyond the political. Discourse is desecuritising, therefore, we must push for debate on every digital issue.

While it is tempting for conceptualisations of network desecuritisation to embrace delusions of cyber-utopianism (the belief that the culture of the Internet is inherently emancipatory) or Internet-centrism (the belief that every important question about modern society and politics can be framed in terms of the Internet), freeing the network does not necessarily translate into a free world. The political has always been both passionate and subjective. It is naive to think that the Internet can save us, and it is similarly naive to think that it can ruin us. As Morozov (2011) points out, for better and for worse, the world has arrived online, and busied itself with everything from looking at cute pictures of cats and tweeting movie reviews, to building encyclopaedias and distributing classified diplomatic cables. If there is hope, it lies in a self-acknowledgment regarding what it is that we actually fear, desire, and believe. It lies in pushing, questioning, and critiquing current speech-acts, past securitising moves, and all the rhetoric surrounding the Internet, in order to keep the network within the public discourse. This does not mean that the network can or should ever be totally free, just that a democratic dialogue must be a prerequisite before policy is ever drafted in the first place.

Conclusions

While there is still a digital divide to bridge before the Web is truly a global technology, the Internet has given more individuals increasing amounts of power in a shorter period of time than any new development in history. Unlike many other world-changing technologies, there is no institutional barrier to access. This has made it, on balance, mostly destructive of institutional authority, especially that of nation-states and their corporate entities (Gross 2012). Sovereignty encompasses many powers, but one of its core elements has been a monopoly on the control of overwhelming force. Now that hackers are able to penetrate computer networks, such a monopoly no longer exists. Nation-states, not surprisingly, are staunchly resisting the erosion of their power and are seeking ways to reclaim it. Last year, Russia, China, and other malleable allies proposed a U.N. General Assembly Resolution, which failed, suggesting the creation of a global information security code of conduct, asserting that policy authority for Internet-related public issues is the sovereign right of states, and showing that governments seek to tie people's real names and identities to online activity. Additionally, new ways to regulate the Net – such as the now infamous American-based surveillance program PRISM, the Trans-Pacific Partnership, or the Anti-Counterfeiting Trade Agreement (ACTA) – will continually be championed by governments as solutions to "terrorism" or "piracy." Consequently, we must never lose sight of the fact that first and foremost – states want international law to authorise national encryption standards, thereby legalising government surveillance (Gross 2012).

These efforts to control Internet content are growing in scope, scale, and sophistication worldwide. Moreover, the methods used by states to filter content demonstrate a systematic lack of accountability and transparency. Although at first glance these trends may be attributed simply to the strategic interests of states to control information flows across their territorial borders, the policies and practices of Internet content filtering – in particular the use of computer network attacks and offensive information warfare, suggest a much deeper geopolitical struggle over the Internet's architecture that is only beginning to unfold. Just as the domains of land, sea, air, and space have all been gradually colonised, militarised, and subject to institutional competition, so too is the once relatively unencumbered domain of cyberspace (Deibert 2008). This is not to say that some of the censorship occurring is not fully justifiable in a liberal-democratic conceptualisation of governance. Child pornography, human trafficking webpages, identity theft sites, xenophobic and genocidal forums, these are desecuritised norms that the majority of network subscribers would no doubt debate and advocate to be restricted.

The issue is not macrosecuritising all aspects of the Internet *per se*. Rather, it is that securitising speech-acts take the network out of the public discourse in which a democratic dialogue can take place. Therefore, the network needs to be desecuritised by questioning and exposing all securitising moves and speech-acts, critiquing what are officially defined as referent objects and existential threats, leaking and sharing whatever invasively collected data we can get our hands on, and using our critical collectivity to bring the future of the Information Superhighway into an arena where practices such as content filtering and packet shaping are openly contested and publicly deconstructed. The time is now to draw the line and engage in the struggle for a freer Internet – which if that is lost, will be impossible to recover. Failure to act and to fight is unfathomable, because closed censorship of the Internet translates to an Orwellian future devoid of open-information, agency or digital freedom. A future in which we are truly ignorant regarding our oppression because it is digitally concealed and obscured from us, for in the words of the discerning Jeremy Bentham (1840: 152), "as to the evil which results from a censorship, it is impossible to measure it, for it is impossible to tell where it ends".

References

Aradau, Claudia. 2004. 'Security and the Democratic Scene: Desecuritization and Emancipation.' *Journal of International Relations and Development*, 7 (4): 388-413.

Blake, S.,1998. *An Architecture for Differentiated Services*. Washington D.C.: The Internet Society.

Behnke, Andreas. 2006. 'No Way Out: Desecuritization, Emancipation and the Eternal Return of the Political – A Reply to Aradau.' *Journal of International Relations Development*, 9 (1): 62-69.

Bentham, Jeremy. 1840. *Theory of Legislation, Volume I*. London: Weeks, Jordan, and Company.

Bigo, Didier. 2002. 'Security and Immigration: Toward a Critique of the Governmentality of Unease.' *Alternatives Journal*, 27 (Supplement): 63-92.

Buzan, Barry, and Hansen, Lene. 2009. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Buzan, Barry, and Wæver, Ole. 2009. 'Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory.' *Review of International Studies*, 35 (1): 253-276.

Buzan, Barry, de Wilde, Jaan, Wæver, Ole. 1998. *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers.

Campbell, David. 1998. *Writing Security: United States Foreign Policy and the Politics of Identity*. Minneapolis: University of Minnesota Press.

Deibert, Ronald J. 1997. *Parchment, Printing, and Hypermedia: Communication in World Order Transformation*. New York: Columbia University Press.

Deibert, Ronald J. 2003. 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace.' *Millennium*, 30 (3): 501-530.

Deibert, Ronald J. 2008. 'The Geopolitics of Internet Control: Censorship, Sovereignty and Cyberspace,' in Andrew Chadwick and Philip N. Howard, (eds.) *Routledge Handbook of Internet Politics*, New York: Routledge.

Deibert, Ronald J., and Rohozinski, Rafal. 2010. 'Under the Cover of the Net', in A. L Clunan, and H. A. Trinkunas (eds.), *Ungoverned spaces: Alternatives to State Authority in an Era of Softened Sovereignty*. Stanford, Calif.: Stanford Security Studies.

Deibert, Ronald J., and Rohozinski, Rafal. 2012. ‘Contestinf Cyberspace and the Coming Crisis of Authority’, in Ronald Deibert, John Palfrey, Ratal Rohozinski, and Jonathan Zittrain (eds.), *Access contested: Security, identity, and resistance in Asian cyberspace*. Cambridge, Mass.: Ottawa: MIT Press.

Gandy, Oscar. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder: Westview Incorporated.

Gross, Michael Joseph. 2012. ‘World War 3.0.’ *Vanity Fair*, May, 2012.

Goldsmith, J. 1998. ‘Against Cyberanarchy.’ *University of Chicago Law Review* 1199 (3): 1217-1222.

Hansen, Lene. 2000. ‘The Little Mermaid’s Silent Security Dilemma and the Absence of Gender in the Copenhagen School.’ *Millennium*, 29 (1): 285-306.

Huysmans, Jef. 1998. The Question of the Limit: Desecuritisation and the Aesthetics of Horror in Political Realism.’ *Millennium*, 27 (3): 569-589.

Huysmans, Jef.,2006. *The Politics of Insecurity: Fear, Migration and Asylum in the EU*. London: Routledge.

International Telecommunication Union (ITU). 2009. *Internet Indicators: Subscribers, Users and Broadband Subscribers*. Washington D.C.: Decade Analysis.

McSweeny, Bill. 1998. ‘Durkheim and the Copenhagen School: A Response to Buzan and Wæver.’ *Review of International Studies*, 24 (1): 137-140.

Morozov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs Books.

Nunziato, Dawn C. 2009. *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age*. Stanford, California: Stanford University Press.

Palfrey, John., and Zittrain, Johnathan. 2008. ‘Internet Filtering: The Politics and Mechanisms of Control’, in Ronald Deibert, John Palfrey, Ratal Rohozinski, and Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*. Boston, Massachusetts: The MIT Press.

Pariser, Eli. 2011. *The Filter Bubble: What the Internet is Hiding from You*. New York: The Penguin Press.

Peoples, Columba, and Vaughn-Williams, Nick. 2010. *Critical Security Studies: An Introduction*. New York: Routledge.

Potter, E. H. 2002. *Cyber-diplomacy: Managing foreign policy in the twenty-first century*. Montreal: McGill-Queen's University Press.

Rosenau, J. N., and Singh, J. P. 2002. *Information technologies and global politics: The changing scope of power and governance*. Albany, NY: State University of New York Press.

Singh, J. P. 2007. 'Meta-Power, Networks, Security and Commerce', in Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel (eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Aldershot, UK: Ashgate.

Singh, J. P. 2010. 'Negotiating Internet Governance', in A. L Clunan, and H. A. Trinkunas (eds.), *Ungoverned spaces: Alternatives to State Authority in an Era of Softened Sovereignty*. Stanford, Calif.: Stanford Security Studies.

Swiss, Thomas. 2000. *Unspun: Concepts for Understanding the World Wide Web*. New York: New York University Press.

Wæver, Ole, Buzan, Barry, Kelstrup, Morton, and Lemaitre, Pierre. 1993. *Identity, Migration and the New Security Agenda in Europe*. London: Pinter.

Wæver, Ole. 1995. 'Securitisation and Desecuritisation', in Ronnie D. Lipshutz (ed.), On Security. New York: Columbia University Press.

Warf, Barney. 2011. Geographies of Global Internet Censorship. *GeoJournal*, 76 (1) 1-23.

Williams, Michael C. 2003. 'Words, Images, Enemies: Securitization and International Politics.' *International Studies Quarterly*, 47 (4): 511-531.

Wilson, Ernest J. 2009. 'What Is Internet Governance and Where Does it Come From?' *Journal of Public Policy*, 25 (1): 29-50.