

COMMUNICATIONS WITHIN GLOBAL SPACE:
Negotiations of local/global tensions within the computer antivirus industry

Jessica Johnston
American Studies Programme
School of Culture, Literature and Society
University of Canterbury
Christchurch
New Zealand



Presented at
The Annual Meeting of the Australian and New Zealand Communication Association
Christchurch, New Zealand
4-7 July 2005

Abstract

Based on qualitative interviews with international computer antivirus researchers, computer antivirus vendors, and IT administrators responsible for managing antivirus software, this paper will explore the politics of communication within their international market place. The computer antivirus industry is seemingly united in its portrayal of itself as having a public responsibility and civic duty to protect and serve the naïve and unwitting computer user. The image they promote is one of a cohesive global crusade against the disembodied computer virus writers, cyber terrorists and spammers and their malicious production of “malware”. Within this obvious marketing crusade though, there are tensions among industry players on “proper” methods, techniques, and goals. Reflecting and reproducing national ideologies and tensions on an international stage, divisions arise as the threat of cyber terrorism intensifies, and speed of the global spread of viruses and spam increases. Accusations and allegations are whispered and repeated about Israeli promotion of misinformation, about government interference in China, about the EU stealing Russian software, about the corruption of Japanese students, about US cultural imperialism, about al Qaeda and the risks of cyber terrorism. This paper will theoretically analyse the assumptions, reproductions and negotiations of cultural identities within the global marketplace of the computer antivirus industry as industry players attempt to both cooperate and compete for market solutions against the increased threat of computer viruses, spam and cyber terrorism.

Introduction

Computer security rhetoric draws upon semantic superimpositions of embodiment, sexuality, global capitalism and citizenship. Through these discourse topics, information technology (IT) professionals draw analogies between infections of biological viruses and threats to the nation-state and global currency flows. This paper will analyse security experts’ discussions of intrusions to computer networks – viruses, denial of service attacks and spam as constructed through contestations around threats to the embodied computer, to ‘the nation,’ and to the global networks within advanced capitalism. Specifically, it will explore the intersections between communication theory, theories of globalisation, and science and technology studies, analysing how the globalisation processes facilitated by new communication technologies reflect and influence negotiations and contestations surrounding international computer security. The computer antivirus industry provides evidence of a transformation into a singular homogenisation of socio-economic or cultural space. Yet the research also reveals that geography and ‘the nation’ still matter in a very real sense as local and national geographical specificities continue to shape technological discourses. The social articulation of these differences though is a complex, on-going negotiation. The deepening internationalisation of the economic structures imposes new constraints on certain kinds of national-level economic and industry strategies. In the advanced industrial world of computer viruses, talk about computer security both reflects and influences the global restructuring of the nation-state, especially after September 11th.

Method

While some scholars have suggested that globalisation is reshaping individual subjectivity (Bauman, 1992, 1997; Beck, 1992), little empirical research to date has investigated the ways individuals experience and understand ‘the global.’ For this paper, my approach has been to look at how negotiations by computer industry professionals mobilise strategies around ethno-national identities and to search out those areas where contesting ‘national imaginaries’ (Said, 1978) collide. This essay stands then, as a case

study, as an example of how to look at the engagement of cross-cultural/international logics as experienced within a global technology industry. It is an attempt to bridge the gaps in the communication theory about globalisation and technology by examining the discursive constructions of high tech industry professionals. I interviewed IT professionals, predominantly male, within the antivirus (AV) industry at their conferences in Europe, Asia and the United States, at large and small universities and city councils, and at banking and government institutions. They were variously located within the computer security industry¹, including specialist antivirus researchers, developers and vendors of antivirus software, and corporate IT administrators. In total, I interviewed 30 people over a two year period, both before and after September 11th.

Embodied metaphors of contagion

The security professionals I interviewed discuss computer viruses using analogies drawn from biological viruses. They describe the need for individual or networked computer protection in language borrowed from immunology, and in terms that envision computer systems as self-contained bodies that must be protected from outside threats. These discussions often import from popular and medical discourse ideas and anxieties about sexual contamination in populations, and sometimes proffer 'safe sex' tips for computer use. Two security experts, one attached to a large city council IT department and another working at a large university, highlight this sense of contamination. The first illustrates how he discusses the importance of computer viruses with his staff:

Corporate IT manager 1: Well, I tell them it is always good to practice safe sex, but basically you know, you kind of.... if you can explain how a virus works in the human body then you can give rough analogies as to how it works in the computer. And in much of the same types of care that you need to take if you're single on the dating scene sort of thing, where to prevent from, you know, physical contagion, also applies in terms of protecting yourself from an unwanted influence on the computer.

Corporate IT manager 2: Well, computers viruses are like more biological viruses. If people sleep around you're going to get a virus and the computer's the same. If you're passing discs around you're going to be vulnerable and of course you don't know where the other person has had their disc. (Laughs)

Both these managers identify the threat of contagion, drawing a direct connection between the human body and the computer. Individuals/systems begin as pure self-contained entities, but external 'unwanted influences' can corrupt a previously 'pure' and uncontaminated system. In order to protect themselves and their systems, both IT

¹ The computer antivirus industry is considered by many to be a subset of computer security in general. . Some of my interviewees were not antivirus specialists, but were responsible for computer security in general within their organizations. Most of my interviewees used the industries interchangeably. Following their lead, I too will use the terms interchangeably.

administrators suggest people should assume individual responsibility to keep the embodied systems clean through defensive actions against both strangers and even seemingly trusted relationships.

The panoptic power of the 'safe sex' metaphor is obvious. The IT professionals identify the subject's position as corruptible, describing both the individualised and net effects of these infectious interrelationships. Within the network, actions are monitored and traceable to specific points within the potentially all-seeing circuitry. The 'safe sex' metaphor potentially generates docility as individuals are told to police their own actions when connecting sexually and/or with net exchanges.

Through this networked interaction, the body itself is simultaneously highlighted and dispersed. These IT professionals refer back to the body to generate discipline through metaphors of contagion and disease. Threat to the physical body is the point of reference for controlling end-users. The simulation of networked disease is prefaced on the understanding of embodied contagion.

This duality of the networked vulnerable body/computer challenges much of postmodern theory on the body and technological theory that 'leaves the meat behind.' In interactions with members of the AV industry, the body is always already there (Sobchack, 1998). Postmodern theories of technology usually omit the 'reversible relations' and the inherent ambivalence between grounded embodiment and a sense of dispersal within the connectivity. Technologies are transformative and do create new spaces for the body. However, these technological interactions are also grounded in phenomenological experience. Bodies are never entirely transcended. In interaction with others, both IT professionals quoted above identify how each individual's body/computer is vulnerable and needs to be aware and cautious about what is inserted into their personal systems in order to prevent potential dangerous infections, infections which ultimately affect the rest of the interconnected global population. Both the individual's body and computer are susceptible through the act of interactive communication.

Significantly though, it is within this communication with others that the spatial frames between individuals collapse. At the macro level, through the sex and networked communication metaphor, individuals become one of many - connected, 'jacked into' and networked within multiple systems. In the specifically networked global state, the action of connecting allows the end-user to be both everywhere and nowhere. While on the net, end-users are constructed as one point in the circuit, personally vulnerable and able to infect others, and thus simultaneously fluid, multiple, fragmented, and dispersed.

Dispersion & Dangerous Infection

It is this networked sense of fluidity and dispersion where the internet transgresses the limits of the print and broadcast models of communication. Through providing the potential for instantaneous interactive global contact, people are inserted - or insert

themselves - into a machine apparatus that is instantaneously exchanging bytes of information. Individuals become a point *within* a circuit, a circuit that is always open to the world, 24/7, and of course always potentially infecting. Another IT manager discusses infection by his foreign customers:

Corporate IT Manager 3: *They come over here, they plug it in the network or they share their document or they place it up on the internal network and then bang everybody's got it. And it doesn't take long and of course you get not just one virus but multiple viruses...*

The effect of individual contagion within the circuit is on the entire integrated networked system. The speed and global nature of the attack is what fuels the need of and energy driving the computer antivirus industry.

Researcher 1: *Say an AV company in Peru ... if they see something, it's not only going to be limited to Peru. If there are companies in Peru who have been hit by that virus, by the time the Peruvian company gets a sample, that sample comes from business that have US and European and probably Spanish e-mail addresses in their address book... So it has already left the country. And you are never ever going to get ahead of it because it is out of, you know, it has bolted, it's out the stable door. But you can reduce the eventual spread of it because these things always spike fast and die quickly and what we can do is we can make them die quicker.*

While Peru is identified as 'the local', it is used as a place marker to highlight the speed and global nature of the problem. It is here the panoptic AV companies can observe the individual circuits being attacked. It is here that a 'mass mailer' infects the local system, moving from the individual out to the global network, the network in this case defined as the US, the EU, and Spain. Focusing on the individualised countries and their relationship within the network, it is the pace and spread of contagion, and the potential globalised effect that is illuminated with the metaphor of uncontrollable, frightened horses escaping from enclosed safety. The potential for global contagion is used in contradistinction to the job of the AV industry to contain the escaping virus, killing it quickly, and preventing individual infections turning into global chaos, all within a brief time frame.

This quote also highlights how spatial and temporal practices are a never neutral part of a discourse (Harvey, 1990, p.239). Space and time are symbolic processes (Soja, 2000; Munn, 1992, p.116) which are fully implicated in engaging, constraining, producing, and maintaining discursive practices. Within the AV industry, Nancy Munn's (1992) claim is instructive: 'Control over time is not just a strategy of interaction; it is also a medium of hierarchic power and governance' (Munn, p.109). In the AV world, the seeming global spread of a virus necessitates the very existence of the AV industry, while also defining the significant power relations within the industry. At the very foundational level, small or new AV companies who cannot monitor the world networks 24 hours a day, 7 days a week cannot compete when a virus outbreak begins. Having the necessary capital to support transnational offices working 24/7 is a major investment, leaving only large, transnational organisations within the industry competing against each other.

CARO: Urgency, Power and Security

CARO is an acronym for Computer Anti-virus Research Organization. It is a very elite group of AV computer researchers created by the researchers themselves out of the necessity to share specialised, restricted and what they consider to be dangerous information. CARO was initially organised by virus researchers from competing vendors in order to voluntarily 'pool' their knowledge and cooperate on solving virus threats during an outbreak. One veto among the, at present about twenty members, means a person is not elected into the organisation. Reflecting the industry's clientele, CARO membership currently consists of only one woman, and no representatives from Asia or Africa.

Even though they are employed by competing vendors, these researchers cooperate with each other, communicating daily through personal emails and email lists. They are seen by many within the industry as separate from, even above the everyday commercialised politics of the industry. Commercial competition, competing against each other as individuals for a competitive technological advantage is eliminated and replaced by a sense of community and friendship that streamlines the processes needed to operate in the crisis situation of a virus outbreak. A CARO researcher commented:

CARO Researcher 2: The very serious research which is done critically when the big new problem occurs, that's usually done within CARO as a community service. And we all share the information and benefit from that. It also means that we will have the solutions within the smallest time frame possible rather than having to do everything by yourself and then have to wait three, four months before you have found everything.

CARO solutions are collectively researched, both reactively and proactively in an attempt to anticipate current and future outbreaks. Although CARO's collective expertise is important for the actual analysis of a 'virus string', because of its limited and highly selective membership, it is not an effective or efficient way to contain the initial 'spike' stage of a virus outbreak. CARO can be seen as the pinnacle of the hierarchy within the industry – twenty dedicated white men, and one woman, from the US and Europe who share highly dangerous and contagious virus samples with each other exclusively, working hard at predicting and staying ahead of virus writers. The information the CARO researchers generate though, is more problem-based and less responsive to the immediacy of a global attack. It is consequently less effective at rapidly publicizing virus alerts or containing virus attacks.

REVS (Rapid Exchange of Virus Samples) on the other hand, was an organisation started by a groundswell of frustration fuelled by the lack of information distributed from CARO when an actual global virus broke. REVS was an organisation of AV *vendors* who shared information about viruses and virus outbreaks with each other. If a vendor noticed a 'spike' in reports of an incident, REVS facilitated an 'early global warning' system to all the other vendors by sending copies of the virus to all members in the entire association. A CARO member who was against the formation of REVS comments about the lack of control when sending a virus sample to the REVS e-list:

CARO Researcher 3: *[When you send messages] to the mailing list provided by the company, it means that that if you send them the virus, anybody, any of the members will receive it. Now imagine that some problem as occurred, for instance a company X who is a member has behaved unethically. With the structure of REVS, the only choice you get is not to send the virus to anybody. Membership should be individual not company based.*

According to this CARO researcher, only individuals can be trusted and held responsible to receive a 'live' computer virus. REVS as an organisation was vendor based, harbouring a potentially unethical unknown individual, thus furthering the infectious likelihood of an outbreak. Because of this potentially infectious state, many CARO members refused to send virus information to any organisation that was part of REVS. This action ultimately ended the existence of REVS. People and organisations could not afford, literally and symbolically, to be out of the CARO information stream. The need to disseminate urgent and vital information about a global virus outbreak was repositioned by CARO as a dangerous attempt to spread secret information to untrusted and potentially unethical 'anybodies.' REVS' discourses of time and urgency were trumped by associated trusted networks and the power to control informational flow. Significantly, another organisation AVIEN (AntiVirus Information Exchange Network) was started a few months after the disbanding of REVS by a group of system administrators from large global corporations who were frustrated waiting for information about virus outbreaks from their vendors. These corporate IT professionals agreed to share information about outbreaks between themselves. Though some CARO members have fought its existence, because of the global nature of the large corporations, and the transnational clout of the original system administrators who started the organisation, AVIEN seems to have been accepted.

Corporate IT Manger 4: *I think AVIEN's the best thing that's ever happened to the communication. There is definitely a lack of getting information to those of us in the field, those of us you know, trying to protect our company. We weren't given information in a timely manner at all, even if it was from our own vendors. And now, and more often than not, we're the ones that are seeing things first and so it's – bottom line, my job is to protect my company and that's my priority. And I need to know what I can do, whether it's something proactive or just mitigate something until there's protection in place, I need to know that. AVIEN gives me that option now because – and it's given me a communication tool that did not exist and it's just opened up, I think, a lot of exchange that needed to be done.*

Increasingly, corporate users of AV products are demanding greater voice and control within the AV industry, touching on questions of how different 'needs' and 'services' and 'securities' are defined, and how, and by whom, industry objectives are set and pursued. As this corporate IT manager illustrates, it was the lack of information about the spread of viruses and the non-'timely manner' with which that information was received which threatened his company. In fact, he suggests that the corporations are the first ones to notice attacks on their systems. Being first in the chain, communicating the observation

of an attack to other corporations in AVIEN can lead to ‘proactive’ or ‘mitigating’ containment options. AVIEN has led to a more direct global communication between potentially infected corporations. AVIEN members no longer rely on CARO or their own vendors to notice a ‘spike’ in network activity, and then wait for the researchers to determine the type of threat and what should be done. Instead, they see themselves as ‘on the frontline.’ When they receive an AVIEN email message from one of their corporate members about a ‘spike’ in their network action, each corporate IT administrator then has the option to lockdown his network exchange, thus preventing more infections within the corporation, and the global spread of contagion to other corporations on the network. With the global pace of information flow and the speed at which viral infections occur, AVIEN’s corporate based resistance effectively challenged the elite power and control CARO had within the industry. AVIEN has the ability to instantaneously and globally react to network security threats.

Globalisation

Integral to these power plays within the AV industry is the use of ‘Global English’. Everyone I talked with, except one Asian AV CEO/researcher, spoke English. Significantly, he has not been invited to join CARO because he would have to rely on a translator, and the translators are not personally known to the CARO members. While many members of CARO are not native English speakers, all meetings, all internet correspondence, all ‘official’ communication is done in English. At AV conferences in Europe and Asia all presentations and social events are in English. Not speaking English is considered a drawback.

Vendor 1: I have difficulty finding technical people in companies in the Far East who speak English, sometimes the only people you can find in companies in the Far East are the marketing people and that's obviously a bit of a problem from what we are trying to do.

Viruses however, are not impeded by translation issues:

I: Do viruses stop because of language problems or do they increase?

Vendor 2: In a purely technical sense, some of them might do because they don't happen to work on different platforms. But most of them don't stop. No, if they are carefully done or sufficiently lucky they just go right on through.

If viruses are ‘carefully done’ or ‘lucky,’ translation into a universal technical language accelerates their global spread. While the lack of understanding of different languages is recognised as hampering both the ease of virus transmission and the smooth communication between industry professionals, the domination of the English language for communication is unquestioned and reproduced as the collective language of the AV industry. According to AV industry’s practice, Global English is the language of net business, and thus also the language of computer security.

But with China increasingly participating as a global economic force, can English serve adequately as the basic language of the internet? With China also becoming known as the centre for internet piracy, how will computer security adapt? How universal then is this

Global English? If language is a system of signs of a language community, who is in/out of the community of Global English?

Global English is used in spite/because of the transnational environment of all AV companies. Reflecting the global dispersions of internet threats, the focus of AV companies' business orientation is beyond the nation-states within which they live/work. Connected with the use of Global English and these transnational connections is the perspective that one state, or one nation alone, cannot address the threat posed to the globalised networked technologies. 'The State,' traditionally defined in relation to the geopolitical territory it governs, is re-imagined by those in the AV industry to justify the application of laws that extend beyond its jurisdiction into the non-territorial, extra-sovereign space of the internet. This international space becomes a new global place that needs protection. The State is seen as a partner in a collaborative effort to battle international cybercrime. The cooperation between the AV industry with various governments after September 11th is the most obvious example:

I: September 11th. Did that have an effect on the industry?

Vendor 3: It definitely changed the legal environment because a lot more countries went and ratified and created the laws against electronic warfare, against virus writing which is good, which is very good. I want to see more consolidation here as well. I want consistent laws between the countries so that [terrorists and virus writers] don't feel safe in any of the countries. So, I want the virus writing to be outlawed like uniformly everywhere.

This construction of the transnational, bureaucratic network of consistent international laws goes hand in hand with the use and expectation of Global English and the changing definitions of security. Because of information technology's instantaneous global communication potential, it has become instrumental in the development of connections between threats to global security and public safety. The AV industry uses discourses identifying the figure of the 'enemy' and the relationship between 'us' and 'them,' generating an artificial homogeneity and simultaneously, a secured space for international corporate business interactions. After September 11th, the French, UK and the US governments all stepped up their security and prosecution efforts against cyber terrorists. As a result, global cooperation between AV companies and national governments are linking global issues of economic management, with policy formations on internet security. The domestic and international become fused spaces through a series of interlinked processes: of domestic and foreign economic policy, transnational business and trade, and the passing of consistent international laws and prosecution.

CARO Researcher 3: On the angle of laws for instance, the spam laws and the effort towards making global hacking laws and things like that, the EU has been stepping up with some of those so it's interesting to see how they're addressing

things... We all recognise that ultimately we need a single law, or something that is relatively the same all throughout the world or it is just going to be a big mess.

In an age of electronic commerce, 'malware' is viewed as a threat to the integrity of the virtual marketplace and transnational commerce flows. Security professionals have begun to speak of computer systems as requiring defence protocols and global laws in order to arrest and prosecute the new type of malware writers, from millionaire spammers to the Russian mafia.

At the most basic level, the AV industry's foundation is to protect and secure capital. Technological advances and the job of marketing and raising capital for that technology are entwined. One vendor discusses the necessary transformation that any successful AV vendor, even one in Eastern Europe, must address in order to survive within the industry. He suggests that any creative technical solutions for computer security or an exclusive focus on the technology must adapt to accommodate a basic rudimentary commerce orientation:

Vendor 3: No one wants to become a 'capitalist' from Eastern Europe, because they don't believe in capitalism, they don't believe in marketing, they don't believe in all this PR hype. For them to have the 'Golden Egg,' and say, 'I have the "Golden Egg" and all of the people who use our product have it,' ok? So this minuscule little population over here has that ok? But because of their ideology, they'll not allow the rest of the world to have it... But don't tell me that you're completely committed to stopping the virus problem when you're not allowing what it is that you have to be offered up to the rest of the world.

Developing capital is seen as necessary within a global economy of the AV world. While good ideas and personal trusting relationships are part of the AV industry, according to this vendor, the Eastern European AV engineer must develop/advance his 'golden egg' and become a global capitalist in order to contribute to 'saving the world' from malware. By choosing not to promote his product, the non-capitalist Eastern European engineer is constructed as naïve and selfish, his ideology and principles dismissed as irrelevant, his geopolitical location in Eastern Europe collapsing geography into/political ideology.

This discourse functions to promote and legitimate the prevailing corporate ideology of globalisation within the AV industry. Within their desire to protect the world from the threat of contagion, globally 'stopping the virus problem,' they must capitalise and promote a product. The global market is intimately woven into the AV industry's basic perimeters.

I: The internet, does that kind of take away the sense of the global boundaries?

CARO Researcher 4: Yes, the only global boundary there is now is the world. I just read that Zambia was connected to the internet as the last country in South Africa, so the world is connected to the internet now and that means, you can do,

I mean, right now I am ordering my DVD's in Australia because of the low Australian dollar, it's cheaper, so I mean, for me it's the same effort to order a Dutch shop, or a US shop or an Australian shop, I just go to one web site buy it and then it's done, so there are no boundaries any more here.

I: Is that a good thing or a bad thing?

CARO Researcher 4: Information-wise it's a good, because you can find all the information you want on the internet. On the other hand it is opening the world as well for the world wide attacks. Any... I can attack any system in the US, the denial of service attack, and it can be to CNN.com in the US, and it can originate from Asian countries, only because there is no boundary any more.

It is as though the logic of the deregulated market has found its perfect instrument in the Web. This AV researcher articulates the formation of a new techno cape that makes the speculative idea of an all-encompassing political economy – and unitary world civilisation – seemingly a commercialised reality. He is the ultimate global consumer. He appreciates the dot-coms of a borderless world for its convenience and prices. In sum, digitalised capitalism promises a reconstruction of the nation-states as an electronic global consumer village. The lack of boundaries identified within his quote is a lack of boundaries for globalised sales.

As this researcher identifies though, there is a 'dark side' to this globalised networked access. The entire 'global village' is 'open' and thus at risk of attack from anywhere within the village. The centre of US corporate news and information is also vulnerable to an assault that can originate from 'Asian countries.' The technology is seen as positively contributing to the removal of boundaries between countries, yet this unbounded openness generates risks and vulnerabilities that need to be contained by more technology. Inherent within the unbounded structure of internet communication, is the construction of tensions between East and West, constructions of potential attacks from anonymous 'others.' The unbounded nature of this global consumer village is also the problem, as malware is also easily accessible and transmitted around the world.

Nationalism

As researchers' and vendors' quotes above indicate, the AV industry is both a product and promoter of economic, market, and political globalisation. The AV industry is charged with policing a world order for 'friction-free capitalism,' of transnational mobility and network connectivity. Those interconnections though also exemplify the tensions between globalism and nationalism and provide fertile ground for articulations of national identities. The researcher above identifies that there is the growing sense among those who operate within this transnational world that this global communication space is rendering obsolete the old order of national territories and boundaries. Yet even within the AV industry and a technocultural discourse that promotes and legitimates the prevailing corporate ideology of globalised capitalism, national identities are not being transcended. Instead, like the body/computer metaphor, the ambivalences and 'reversible relations' inherent in tensions between nationalism and globalism are articulated. The

globalised corporate business ideals are filtered through national identities. Even though computer viral threats are promoted and become recognised as global threats, the interrelationships between political economy, technocracy, and ‘the other’ become central to computer security as a vector and rationality of power. Eastern Europe, Japan, China, the US and Africa are all differently identified as ‘other’, yet depending on one’s geopolitical position, all these nations are conceptualised as outside the security nexus:

Vendor 5: The Japanese market is (pause) despite what some people may believe, particularly the Japanese, it is very undersold at the moment. There is a lot of gaps, there are a lot of gaps, and there are many companies that are not protected, mainly the smaller companies, but there are many more companies who are protected but not protected adequately...

CARO Researcher 5: Yeah. The only difference was that before 9/11 everybody was talking about China. After 9/11, or immediately after 9/11, the concentration went over the Al Qaeda but after recognizing that Al Qaeda didn't pose a threat there, everybody went back to ...

I: China.

CARO Researcher 5: China. They're not sure about China.

I: Is China a threat or is it hype?

CARO 5: I think China is a threat in the monetary sense and so you think of, well you could use an attack on the internet to, to gain command and some of that. And it's also a closed society so that people don't know what's going on and therefore you have the conspiracy things and you can always blame things on China.

A discussion with two Asian vendors suggested otherwise:

Vendor 6: The problem, where does the problem come from? We can see that there are virus writers, originally it is from the West, we call it the West including Europe and America, OK, all the non-English speaking, even non-Caucasians we believe is, we call it West.

Vendor 7: What an extremely odd thing to say. Didn't Stoned [virus released in 1987] originate in New Zealand? Brain [virus released in 1986] originate from Pakistan?

Vendor 6: Well, yeah. That is why it is original, originally it is believed that it is outside. AV coming in to solve problems, if you look at it.

From the Western perspective Japan is seen as ‘undersold’ and because the AV market is not saturated, this nation has gaps in its computer security and is naively unprotected. China is seen as a financial threat, one that will attempt to ‘gain command’ over the internet. And from the Eastern perspective, viruses originate in the West, ‘outside’ their region, such that their local AV companies must solve these western problems in order to protect their own society.

Through the increased speed and pace of communication within globalised networks, even with the world being defined as a single globalised borderless space, AV professionals in both the East and West have different visions of this global order. The West seems to understand itself as the guardian of universal values on behalf of a world formed in its own image. The East as a self-contained and isolated space, understands that it must protect itself from the intrusion of Western technological inadequacies. So while the intensification of communication flows creates a transnational space, within that space, geopolitical identities are actively reasserted by the people interacting there. To talk about global culture is equally to include these forms of cultural contestation (Featherstone, 1997). In response to the global compression and the intensity and speed of transnational information flows, these AV professionals also articulate de-globalised nationalistic imagined communities, projecting onto the 'other' the attenuating fears around submersion within a global state.

Nations are more than geopolitical entities; they are discursive constructs which by their very nature are acts of inclusion and exclusion. They symbolically delineate membership in the national 'imagined community.' However, discourses of national identity are constantly shifting and constantly shaping and being reshaped by changing social conditions. Japan, China, India, Pakistan, Al Qaeda, the US, the EU are all potential threats to technological order, depending upon one's geopolitical location. What has been left out of any discussion of globalisation is the continent and nations of Third World countries.

CARO Researcher 4: *I mean everybody is always mentioning the Third World countries. These are also the countries we ship our old systems to, the old operating systems with the known holes, which are easy to infect for hackers because [the holes in security] are documented.*

I: *...but again the fixes are there also, yeah?*

CARO Researcher 4: *Yes, but some operating systems cannot be fixed, some holes... Because the machines cannot handle that. All the operating systems will be unuseful... Maybe that's one of the bigger problems that the antivirus industry or security industry should actually give a discount on security products to the Third World countries.*

I: *That's a nice thought. Could you promote that?*

CARO Researcher 4: *I can, but no body would sell there.*

I: *Why?*

CARO Researcher 4: *You're a commercial company. What I do costs money. Somebody has to pay for that and that's the customer.*

This is the world in which networked capitalism functions – the world of electronic transactions, information flows and elite knowledge contestations. As this extended quote

from a researcher indicates, 'the global' continues to be marked by very specific market boundaries on demand and consumption fronts, based around distinct geopolitical identities, because of and in spite of the global production and distribution reach of communication technologies. This is a world where producers of technology reproduce socio-structural hierarchies. Instead of globalisation and internet connectivity eliminating cultural differences resulting in a unified, homogenised global culture, this quote points to the brutal consequences of economic and technological rationales which justify maximizing economies of scale and production. The quote explicates the processes by which global communication technologies are actively shaped within capitalist production and consumption contexts, the important political, economic and social factors which influence organisations to address or ignore diverse technological needs. The quote illustrates how the 'progress' of global transformation is unstable and uneven, and not easily reduced to generalizing terms such as 'de-centering.' When examining the development and influence of technology and the internet on transnational communication flows, attention must be paid to particular 'local' economic, political and socio-cultural processes that shape the extent and forms of those global communication flows. The internet is not a value-neutral entity, but is negotiated through and produced within these systems.

References

- Bauman, Z. (1992). *Intimations of postmodernity*. London: Routledge.
- (1997). *Postmodernity and its discontents*. New York: New York University Press.
- Beck, U. (1992). *World Risk Society*. Cambridge: Polity Press.
- Featherstone, M. (1997). 'Global and Local Cultures.' *Undoing Culture: Globalization, Postmodernism and Identity*. London: Sage Publications.
- Harvey, D. (1990). *The condition of postmodernity: an enquiry into the origins of cultural change*. Oxford: Blackwell.
- Munn, N. (1992). The cultural anthropology of time: a critical essay. *Annual Review of Anthropology* 21, 931-23.
- Said, E. (1978). *Orientalism*. London: Routledge and Kegan Paul.
- Sobchack, V. (1998). Beating the Meat/Surviving the Text, or How to Get Out of This Century Alive. P. A. Treichler et al.. *The Visible Woman: Imaging Technologies, Gender and Science*, New York: New York University Press.
- Soja, E. (2000). *Postmetropolis : critical studies of cities and regions*. Malden, Mass.: Blackwell Publishers.

Address for correspondence

Jessica Johnston
 American Studies Programme
 University of Canterbury
 Private Bag 4800,
 Christchurch
 New Zealand