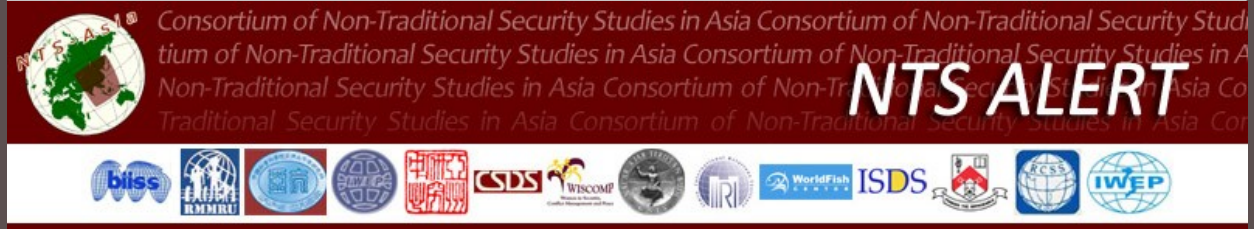


NTS Alert on Cyber Security (Oct/02)

The Final Frontier: Non-Traditional Approaches to Cyber Security

The discourse on Cyber Security, a relatively new field in non-traditional security studies, has been dominated by the need to protect information infrastructure from both state and non-state actors. However, this conception fails to consider alternative definitions of Cyber Security. Alternate conceptions value information access and integrity as equal to the need to protect the confidentiality of information, and allows non-state actors to act as agents of securitisation.

Contents:

The NTS Alert Team

Mely Caballero-Anthony, Nur Azha Putra and Kevin Punzalan.

- Consortium of NTS Studies in Asia
- Centre for NTS Studies

Introduction

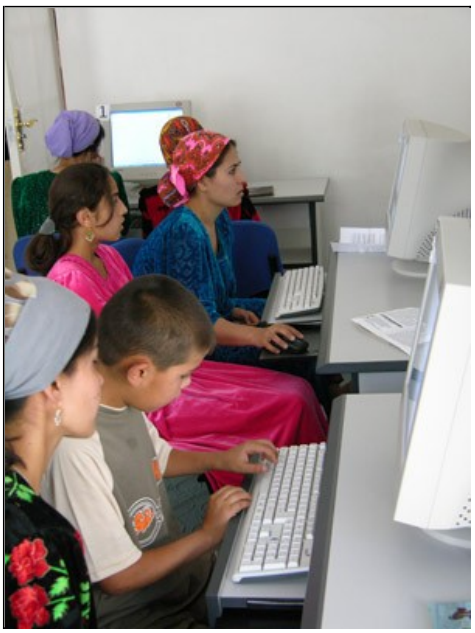
In our previous NTS Alert on Cyber Security, current trends and issues in the securitisation of cyber space were discussed, along with contemporary threats and their potential to disrupt electronic infrastructure. It was pointed out that analysts have begun to consider cyber security as an aspect of national security that must be guaranteed, as illustrated by the cyber attacks on Estonia and Malaysia recently.

These attacks, which so far have consisted of Distributed Denial-of-Service (DDoS) attacks aimed at disrupting information systems, belong to a dominant narrative of cyber security. However, a clearer picture forms when the narrative is analysed through the Copenhagen School's securitisation model. In deconstructing the narratives, the state as the securitising actor identified its cyberspace as a national security concern which therefore requires the allocation of the government's resources to mitigate the threats. Hence, in this narrative, the state's national information and communications networks are the primary referent of security and threats emanate from rogue actors via unsecured global networks.

Despite this dominant narrative, other conceptions exist, which utilise different agents and referents in place of the state and its security concerns. This paper examines the alternative and perhaps contending conceptions of Cyber Security and the corresponding issues.

The Dualistic Model of Technical Computer Security and Cyber Security

Helen Nissenbaum (2005), Professor of Culture and Communication at New York University, illustrated the contrasting conceptions of computer security and cyber security in an article published in the journal *Ethics and Information Technology*. While the two conceptions share similar elements, each model embodies different values. While 'technical computer security' is defined by its goals of ensuring information availability, integrity, and confidentiality through the protection of computer systems and users, 'Cyber Security' is defined by its goals of protecting the state from the use of networked computers for subversive purposes, actual attacks on critical societal infrastructure dependent on computers, and from the threat of network disablement.



Gennadiy Ratushenko /The World Bank

Her model of 'technical computer security', in essence, makes the protection of information the referent of securitisation, and allows a number of actors, including individuals, private institutions such as private internet security companies, the media, and non-government organisational (NGOs) to become agents of securitisation. In contrast, her model of 'Cyber Security' firmly ensconces the state as the sole and primary agent, and elevates the 'national interest' as the referent. The implications of the differences between these two models are profound: While the former model requires that the strength of the various actors affected by breaches of security to strengthen their individual capacities and to reduce their vulnerabilities, the latter model allows the state to justify measures that may curtail the freedom of other actors in the name of national security, including the centralisation of control over networks, technical barricades that restrict access to online information, and mechanisms that monitor and filter information flows.

Table 1 Nissenbaum's conceptions of security

	Technical Computer Security Model	*Cyber Security Model*
Securitising Actors	Individuals, media, NGOs, business, private internet security companies	State, government organs
Referents	Protection of information availability, integrity, and confidentiality	Protection of classified information infrastructure from subversion, disruptive attacks and network disablement
Measures to attain security	Reduction of security vulnerabilities, strengthening of individual security capacity	Centralisation of network control, technical barricades, monitoring and filtering information from users, surveillance

Source: Nissenbaum 2005

Ironically, the Cyber-Security model may enhance network security, but also marginalises the ability of cyber space to adhere to its original role: as a realm of public exchange, as pointed out by Nissenbaum. This in effect increases the security of the state, but may harm the human security of non-state actors who are also end-users of the network infrastructure that the state aims to protect. This point is further developed in the next model to be discussed.

^ To the top

The 'Panopticon': Surveillance and Cyber Security

In essence, the creation of a surveillance regime has helped transpose elements of Jeremy Bentham's 'Panopticon Model' of maintaining discipline onto society itself. While the Panopticon was intended as a system for efficiently maintaining surveillance over prisoners (see Figure 1), it may now be used to characterise a modern 'capitalist surveillance regime'. Richard Fox has suggested that modern forms of surveillance allow the state to not only ensure compliance with laws, but also to allow it to shape and tailor policies based on the information it has collected on its citizens. While it is true that this form of surveillance has not occurred without the awareness or consent of modern citizenry, its collective effect has been to induce 'conformity through deterrence', and to minimise the risks posed by individuals by 'excluding potential rule breakers from opportunities' (Fox 2001). The surveillance regime essentially creates an imbalanced relationship between the state (or private entities) and the monitored individuals, because the latter have little control or knowledge of how information collected on them is used.

Figure 1 A real-life Panopticon model

Source: The Philippine American War, 1899-1902 by Arnaldo Dumindin. Available at <http://www.freewebs.com/philippineamericanwar/thelastholdouts.htm>.

In the process of protecting national security in the case of the state, or pursuing commercial competitiveness in the case of business entities, *passive surveillance has the potential to endanger the security of those being monitored in terms of their right to privacy.* In contrast to the state's referent of national security (an existential prerogative), an individual or organisation being monitored is inhibited from the exercise of freedom of movement, association, assembly and speech (Fox 2001). The prevention of the exercise of these rights impedes human security in both the personal and political dimensions, as outlined by the 1994 United Nations Human Development Report.

However, it is simultaneously impractical and problematic to discount all forms of surveillance as unnecessary, as the state possesses the responsibility to pursue cyber-criminals and to monitor genuine and imminent threats to national security. To accommodate both perspectives, better designed controls on the surveillance powers of the state and private organisations are necessary. Progress on this front remains to be seen, however. As late as April of this year, the director of the National Cyber Security Center at the Homeland Security Department of the United States (US), Mr Rod Beckstrom, resigned over concerns that the National Security Agency would acquire surveillance powers over federal employees, even as these were ostensibly targetting foreign cyber security threats (Risen and Lichtblau 2009). In the same article, the Director of National Intelligence, Dennis Blair, admitted that there had been occasions that the US government had 'intercepted the wrong communications', but did not reveal the scale or frequency of these incidents.

Nevertheless, the expansion of electronic surveillance has greatly increased since the advent of the information revolution. The employment of this tool has become routine, especially in securing sensitive physical infrastructure and in preventing and deterring crime. Surveillance on the internet has also been made possible by legislation which allows national authorities to intercept different forms of electronic communication without legal hindrances.

In 1994, the United States enacted federal laws that required telecommunication agencies to ensure that their services are open to interception by law enforcement agencies. In 2000, the United Kingdom enacted legislation that required companies to install decoding equipment that allowed law enforcement agents to monitor emails on their networks. Government databases may now be interlinked, allowing police databases to share information with other government offices, such as with social welfare or child protection services (Fox 2001).

Ironically, the Cyber-Security model may enhance network security, but also marginalises the ability of cyber space to adhere

to its original role: as a realm of public exchange, as pointed out by Nissenbaum.

At the point of writing, the International Telecommunications Union (ITU) is in the process of drafting an international protocol on cyber security and cyber crime, which was proposed in November 2008. In 2007, the United States ratified the Council of Europe Convention on Cybercrime, which came into force in January of that year. Singapore, Malaysia and Brunei signed a joint initiative on cyber crime on 23 March 2006. Indonesia passed an Electronic Transaction and Information Law in 2005. In the Philippines, a bill on cybercrime was filed in the Philippine Senate in April of 2009 (Schjolberg 2009).

In comparison, the previous model held the protection of information networks and users as the primary referents of security while the current model considers the enforcement of laws and the prevention of cyber crimes as its referents. The state remains important, but private corporations, particularly those that have an interest in protecting intellectual property rights (such as media companies) are also considered securitising actors.

Innovations in communications technology and the outsourcing of government functions to the private sector have allowed the latter to assume powers of surveillance that it did not previously possess. Databases of many large companies collect information on prospective consumers and aim to discern consumer practices. Internet giant Google's AdSense program allows web developers to earn revenue by displaying advertisements tailored to the interests of the visitors of their websites (Google 2009). For example, 'Cookies', a text file utilised by internet web browsers to store personalised information about the user's web preferences, is a form of passive surveillance, which is why internet browsers offer users the choice to disable them (Bennett 2001).

Other examples include the use of credit records, which are stored online and transmitted via credit reference associations, and may be used against individuals with bad credit records from accessing a full array of online services (Fox 2001). Recently, a cyber spying network was uncovered by the Citizen Lab, a think-tank based at the University of Toronto. The network had compromised thousands of computer around the world, many of which were considered 'sensitive targets' such as those located in 'foreign ministries, embassies, news organizations, international organizations, and NGOs. They included the offices of the Dalai Lama, the Russian embassy in Beijing, foreign affairs ministries in Iran and Indonesia, the Indian diplomatic service, and the Asian Development Bank.' (Haggart 2009)

Although these innovations have contributed to greater efficiency in the apprehension of crime in the public sector and the efficiency of marketing and advertising strategy in the private sector, the increase in reach and capabilities of surveillance regimes could potentially compromise the individual's right to privacy as pointed out by Richard Fox. He warned that routine surveillance 'creates an abiding sense of communal unease in which awareness of such scrutiny tends to chill the exercise of accepted civic rights, which include freedom of movement, association, assembly and speech' (Fox 2001). In the private sector, data gathered as a result of passive surveillance of commercial transactions may lead to discrimination against consumers, as in the case of 'dynamic pricing', where prices offered by a retailer differ based on data of customer purchasing habits.

^ To the top

e-Governance: Managing State and Society in Cyberspace

Another aspect of cyber security that merits examination is how e-governance has affected the relationship between the state and society. E-governance is defined as the application of electronic means in the interaction between government and citizens and government and businesses, as well as in internal government operations (Haywood 2002). E-governance is utilised to simplify and improve democratic, government, and business aspects of governance (Backus 2001). An essential function of e-government is the access and exchange of information, which makes interaction between a government and its citizens more efficient, and has the potential to increase the means of political interaction (Jaeger 2005). In addition, information released by government agencies is often viewed by citizens as coming from 'objective authoritative sources', and e-government allows wider and faster dissemination of this information.

E-government, the use of electronic means to facilitate formal and institutional processes that operate at the national level to maintain public order and facilitate collective action (Haywood 2002), can take the form of:

- **Direct email connectivity for public servants,**
- **online forums for espressing opinions and approval on policies,**
- **online transactions for government services; and**
- **networking between different government offices for the sharing of information.**

E-government also has the potential to expand political discourse across a greater range of the population, but this has mixed effects. In the case of Usenet online forums, the expansion of political participation has also led to greater polarisation of views, as the structure of these forums is topic-based, and tends to bring together people with similar views. Their isolation in topic-based forums leads to their isolation from the general public, and thus prevents them from being exposed to critical responses. In the case of the United States, the fact that most people who make use of such online tools come from the American middle class further limits the plurality of the political discourse (BBC News 2009).

Governments themselves may also use their e-government resources to present particular policies in a positive light, using their advantage of being a trusted information source to advance particular agendas even if dissent or opposition to these policies from different sectors of society exist. A particular example was that documented by Paul Jaeger: The website of the American 'No Child Left Behind' Program. While the website of the said program was intended to inform stakeholders and the general public of the details and potential benefits, the way the site was designed was so that none of the drawbacks and costs the program would incur were published online. Because of this, critics viewed the website as partisan and biased towards the program (Jaeger 2005).

With an e-governance framework of securitisation, the referent and agents of securitisation differ according to the political framework of the state in question. 'Closed' or authoritarian systems hold the state as the sole securitising agent, with national security as the primary referent. Here, information and policies flow in one direction from the state to its citizenry, and the implementation of e-

government simply improves the flow of information. In the case of 'Open' or democratic systems, both state and citizenry are securitising agents. The state may identify issues of national importance and disseminate these to the general public using e-governance, while the citizenry may collectively or individually react to these issues and either support or oppose policies, or securitise issues of their own and forward these to the government using the tools of e-government (Parent, Vandebeek and Gemino 2005).

However, it must be pointed out that citizen trust in government, an important issue in democratic systems (and even authoritarian ones), is not directly improved by e-governance. While e-governance may improve the efficiency of information flows and allow citizens of 'Open' systems more space to interact with governments, a study demonstrated that e-governance only improved citizen trust in polities where citizen trust was already stable. Polities with less citizen trust in government recorded negligible improvements (Parent, Vandebeek and Gemino 2005).

E-governance has the potential to improve discourse between the state and its citizens, and to open new avenues for interaction, but this applies mostly to those societies with open systems. In societies that are closed, or where citizens have limited avenues of interaction with the state, the effects of e-governance merely reinforce existing imbalances in political relationships, or may even exacerbate them if the state uses e-government to reinforce policies in a non-transparent environment.

^ To the top

Final Analysis: The Future of Cyber Security

Regardless of the security threats posed by the different permutations of cyber terrorism and cyber crimes, cyber space fulfils the potential for greater cooperation and multilateralism. The international initiatives on combating the influenza pandemic, global disaster alerts and early warning systems on natural disasters are examples of international cooperation in cyberspace.

In fact, in March 2009, the ITU launched its International Multilateral Partnership Against Cyber Threats (IMPACT) facilities at Kuala Lumpur, Malaysia. The new IMPACT facilities host its Global Cybersecurity Agenda (GCA), which is an international framework for cooperation aimed at finding strategic solutions to boost confidence and security in an increasingly networked information society, according to the ITU's press release.

'Cybersecurity is one of the most critical issues of our time...it is a global issue, demanding a truly global approach and it is therefore gratifying to see and to be part of this growing coalition against cyber-threats worldwide. The collaboration with IMPACT complements our efforts in strengthening cyber security and we look forward to expanding the cooperation between governments, the private sector and educational institutions.' said Dr Hamadoun Touré, ITU Secretary-General in the press release.

Security, regardless of its different permutations, should be achieved for all in line with the notion of human security. After all, in the information age, information is the basic commodity.

In a nutshell, Dr Toure's sentiments echoes the general security strategy states are adopting in securing their cyberspace. A tripartite partnership is crucial in ensuring that cyber security is achieved for all stakeholders. However, other non-state actors such as civil society organisations, NGOs and individuals are also consumers of information and technology and appear to have been left out of the mainstream cyber security discourse. Security, regardless of its different permutations, should be achieved for all in line with the notion of human security. After all, in the information age, information is the basic commodity. In the public domain, access to information delineates the line between the information-poor and the information-rich. On the extreme end of the continuum of an information society, the information-rich person makes decisions and are better informed while at the opposite end, the information-poor person is further alienated and isolated. The lack of information may prove to be detrimental especially in an information-based knowledge economy.

Therefore, set against the increasing securitisation of cyberspace, the unintended consequences of a global coalition against cyber terrorism and cyber crime may leave the information-poor person or society increasingly vulnerable as access to information becomes more of a commercial and security concern rather than basic human rights entitlement.

Thus, it is imperative that the formulation of international or national security frameworks on cyber security should include civil society organisations and NGOs in addition to the private sector and educational institutions. The bigger challenge, following this 'expanded' framework, is to strike a balance between national security, commercial interests and human security.

^ To the top

References

Backus, Michiel, 'E-governance in Developing Countries', Research Report, International Institute for Communication and Development, No. 3, april 2001. Available at <http://www.ftpiicd.org/files/research/reports/report3.pdf>.

Bennett, Colin J., 'Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web', *Ethics and Information Technology*, vol. 3, no. 3, 2001, pp. 197-210.

CyberCrime Law website, 2009. Available at <http://www.cybercrimelaw.net>.

Fox, Richard, 'Someone to watch over us: Back to the panopticon?' *Criminal Justice*, vol. 1, no. 3, 2001, pp. 251-76.

Google, *Google AdSense*, 2009. Available at <http://www.google.com/services/adsense_tour/index.html>.

Haggart, Kelly, 'Civil Society Must Get Up to Speed on Cyber Security, Watchdog Warns', The International Development Research Center, July 2009. Available at <http://www.idrc.ca/en/ev-142823-201-1-DO_TOPIC.html>.

Haywood, Andrew, *Politics*, Hampshire: Palgrave Macmillan, 2002.

'ITU's Global Cybersecurity Agenda housed in new centre in Malaysia: IMPACT headquarters in Cyberjaya o focus on strengthening network security', Press Release, International Telecommunication Union, March 2009. Available at <http://www.itu.int/newsroom/press_releases/2009/08.html>.

Jaeger, Paul T., 'Deliberative democracy and the conceptual foundations of electronic government', *Government Information Quarterly* 22, 2005, pp. 702-19.

Nissenbaum, Helen, 'Where computer security meets national security', *Ethics and Information Technology* 7, 2005, pp. 61-73.

'Online politics reserved for the rich', *BBC News*, 2 September 2009. Available at <http://news.bbc.co.uk/2/hi/technology/8233908.stm>.

Parent, Michael, Christine A. Vandebeek, and Andrew C. Gemino, 'Building citizen trust through e-government', *Government Information Quarterly* 22, 2005, pp. 720-36.

Risen, James, and Eric Lichtblau, *The New York Times Global Edition*, 16 April 2009. Available at <http://www.nytimes.com/2009/04/17/us/politics/17cyber.html>.

^ To the top

About Us
The Centre for Non-Traditional Security Studies is a research centre of the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. Please visit the Centre's website at www.rsis.edu.sg/nts/home.html, for more information or email us at NTS_Centre@ntu.edu.sg.