NTS ALERT

October 01/09 Issue

CONSORTIUM OF NON-TRADITIONAL SECURITY STUDIES

A FORTNIGHTLY BULLETIN OF CURRENT NTS ISSUES CONFRONTING ASIA

Compiled, Published and Distributed by

NTS-ASIA Secretariat,
Centre for NTS-Studies,
S. Rajaratnam School of International Studies,
Nanyang Technological University

SECURITY IN CYBERSPACE: THE RETURN OF THE STATE

***Abstract:** The recent cyber attacks on South Korea and the United States, as well as those on Georgia in 2008 and Estonia in 2007 have awakened a certain consciousness in the minds of the international community, particularly that of the security community. As if triggered by a sense of vulnerability, when these cyber attacks managed to disrupt normal services, states were hard pressed to extend national security policies to the realm of cyberspace especially those with highly developed information and communication technology structures. This edition of the Alert traces the securitisation of cyberspace in recent years and ponders its implications for human security.*

CONTENTS

PAGE 2

GLOBAL ISSUES AND POLICY PATHWAYS IN CYBER SECURITY

INTERNATIONAL CYBER ATTACK INCIDENTS

PAGES 3-5

RE-RATIONALISING CYBER ATTACKS

POLICY PATHWAYS IN NATIONAL CYBER SECURITY POLICIES

SECURITISATION OF CYBERSPACE

HUMANISING CYBERSPACE

NTS Alert Team

Mely Caballero-Anthony, Alistair D.B. Cook, Nur Azha Putra and Kevin Punzalan.

Please click below to visit our websites

(1) Consortium of NTS Studies in Asia
(2) Centre for NTS Studies

Contact us at NTS_Centre@ntu.edu.sg

Introduction

The secretary-general of the United Nation's (UN) International Telecommunication Union (ITU), Dr Hamadoun Toure, warned that the next world war could take place in cyberspace. Speaking to stakeholders from across all sectors including heads of state, Dr Toure called for global cooperation across all industries and sectors to provide cyber security which includes the protection of children, businesses and governments. He stressed that cyber security could only be achieved within an international global framework comprising countries who are committed towards protecting their citizens and privacy.

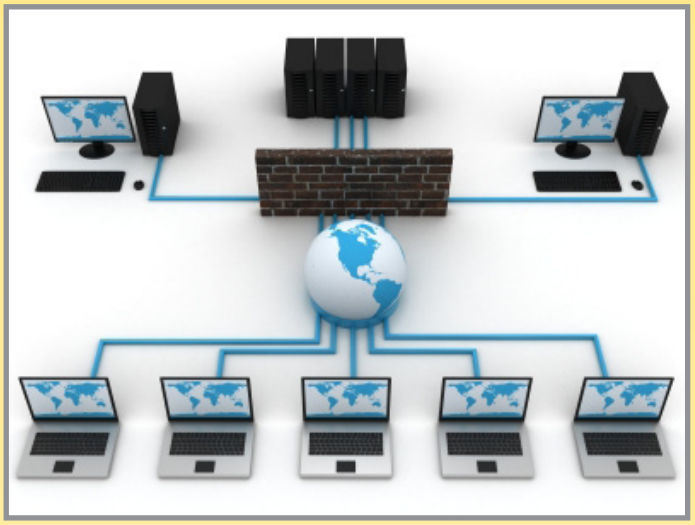
'The next world war could take place in cyberspace and this needs to be avoided. The conventional wars have shown us that first of all, there is no winner in any war and second, the best way to win a war is to avoid it in the first place. So we need to plant the seeds for a safer cyberspace together. And it can only be done at the global level because the criminal needs no longer to be on the crime scene and you can attack many places at the same time in the cyberspace,' said Dr Toure on the United Nations Radio website.

Although Dr Toure's remarks seem alarming, he is not alone. In recent years, the proliferation of cyber wars and cyber crimes have driven multilateral institutions such as the European Union (EU), North Atlantic Treaty Organization (NATO) and the Association of Southeast Asian Nations (ASEAN) as well as national governments such as the United States (US), the United Kingdom (UK), Australia, Malaysia and Singapore towards securing their cyberspace.

Anti-cyber crime laws empower the national cyber security agencies with the legal mandate to protect the state's critical information and communications technology (ICT) networks and infrastructure, particularly from international cyber criminals and cyber terrorists.

The initial phase of delivering ICT infrastructures which drove the transformation from the Industrial Society to the Information Society has

now been coupled with efforts to secure cyberspace. ICT, which was initially meant to reduce the spatial dimension and enhance global communication, has now taken the added burden of national security and sovereignty.



Global Issues and Policy Pathways in Cyber Security

The issue of vulnerabilities and threats posed in cyberspace go beyond those which are politically motivated.

Global internet security giant, McAfee in its 2007 virtual criminology report, *Cybercrime: The Next Wave*, identified three emerging global trends in cyberspace – a growing threat to national security from web espionage, an increasing threat to online services and an emergence of a sophisticated market of software vulnerabilities.

In its latest 2008 report, *Cybercrime versus Cyberlaw,* McAfee highlighted several issues:

- Governments have not given enough priority to cybercrime;
- There is a lack of a transnational law enforcement regime to combat cyber crime which thus impedes international cooperation; and
- Law enforcement at the national and local levels are ill-equipped to cope with increasing cyber crimes especially in digital forensics and evidence collection.

Earlier this year at the World Economic Forum, McAfee projected that companies worldwide have lost more than US $1 trillion in 2008 due to the loss of intellectual property rights and the costs of repairs to damaged data, amongst other things which were revealed in its report titled *Unsecured Economies: Protecting Vital Information*. In particular, the report revealed that cyber mafia gangs are increasingly trying to to infiltrate corporations. Using phishing techniques, cyber criminals target top executives in an attempt to steal vital information.

A 2005 global report by Symantec Corporation, a global information security corporation, showed that Denial of Service attacks grew by nearly 700 per cent. These attacks increased by 119 per day to an average of 927 a day. The largest increase occurred in the small business sector and the education industry. The US, Germany and the UK are the top three locations where these attacks occurred.

More recently, the *Symantec Internet Security Threat Report: Trends for 2008* observed that amongst the threat activity occurring in the government and infrastructure sectors in 2008, malicious activities occured the most in the telecommunications infrastructure sector. China, as a country of origin, accounted for 22 per cent of the total attacks conducted against governments worldwide. This represented an increase of 8 per cent in 2007. The most common form of attack against government sectors was in Denial of Service attacks. Meanwhile, 28 per cent of attacks originated from within the US and targeted the government sectors in Europe, the Middle East and Africa.

Telus Security Solutions, an international internet security firm, pointed out the rising rate of identity theft, increasing vulnerability due to shrinking time between exposure and attacks, increased incidents of spams, the targeting of desktop computers and web-based applications, and new risks stemming from mobility of data. Perhaps, more importantly is the 'professionalisation' of cybercrime. In recent years and perhaps due to the global economic recession, hacking has transformed from a personal hobby to that of an organised criminal business activity. In fact, Telus has singled out criminals rather than terrorists as the main perpetrators of internet-based attacks.

In addition to the proliferation of cyber crimes and cyber espionage, there have been an increased number of alleged incidents of international cyber wars and cyber terrorism.

International Cyber Attack Incidents

In 2007, Estonia was in the middle of a diplomatic dispute with Russia over their removal of a Russian public war memorial. As a result, or by coincidence, the Baltic state came under intense cyber warfare attacks. According to several news reports, these attacks resulted in the disabling of several government websites, newspaper organisations, two of the country's largest banks and companies specialising in communications,. Estonia was especially vulnerable considering that it is one of the most wired countries in Europe.

"Militarisation of Cyberspace in 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace' by Ronald Deibert."

Although the issue of cyber security is not new, political observers noted that there has been an increase in the militarisation of cyberspace especially since 9/11. Deibert for instance, pointed out that, fuelled by the fear of the potential use by terrorists of electronic networks and an 'electronic Pearl Harbour', states have been gradually adopting offensive information warfare capabilities. Drawing upon the theory of the Revolution in Military Affairs, Deibert explained that states have increasingly adopted the innovative use of new technologies and organisation structures as a product of the advances made in the communication and computing technologies. Consequently, cyber war tools such as remote sensing and electronic viruses have led to a major change in the nature of warfare.

According to him, the US is leading the cyber arms race and employs computer hackers, developed advanced computer viruses, worms and Trojan horses and has drawn up guidelines for conducting cyber warfare. The guidelines include establishing the rules and framework within which the US would penetrate and disrupt foreign states'computer systems. Deibert however was unable to cite or refer to any other sources apart from news reports.

Nevertheless, he was quick to point out that many observers are sceptical over the degree of threat involved due to the technological limitation of the ICT architecture, which limits assaults only to the realm of cyberspace and also because of the low pay-off for terrorists whose ultimate aim is premised on physical bodily harm.

Furthermore, Deibert highlighted that there has not been any real evidence of actual acts of cyber terrorism unless one adopts a maximalist perspective and considers any form of hacking and DDoS attacks as attempts towards mass destruction. To Deibert, hacking and DDoS attacks are merely attempts to periodically disrupt internet traffic.

For nearly three weeks, these websites were barraged with Distributed Denial of Service (DDoS) attacks which inevitably paralysed the targeted websites. DDoS is a situation whereby the host computer (or webserver), which houses the targeted website, is unable to respond or communicate with legitimate requests from other computers because its resources have been consumed by the barrage of requests from the attackers. Thus a DDoS attack serves to deny service to other legitimate users by consuming the webserver's resources with an overwhelming number of requests.

A similar attack occurred in Georgia in August 2008 when the former Soviet state was under 'cyber siege'. DDoS attacks were carried out against several government websites following a period of armed conflict between Georgia and Russia over the issue of South Ossetia. The affected websites were those of the Georgian presidential office, Ministry of Defense and Ministry of Foreign Affairs. Interestingly, independent security researchers found that the attacks came from internet traffic which originated in Germany but were re-routed to Georgia via Russia.

In July 2009, South Korea and the US were subjected to three waves of DDoS attacks. According to news reports, a leading South Korean national newspaper and its spy agency were hit by an unnaturally high volume of internet traffic. In the US, the White House and Pentagon were targeted. Perhaps to coincide with the American Independence Day, the first wave started on 4 July, followed by 7 July and finally on 9 July. However, subsequent statements from the affected government agencies and cyber security experts claimed that these attacks, while malicious, were not detrimental as it did not lead to any major disruptions.

Nearer to home, several Malaysian government websites, universities and private institutions were allegedly penetrated by Indonesian hackers during the Malaysia-Indonesia Ambalat dispute in 2005, according to a report by Malaysia's Centre for Maritime Security and Diplomacy. High-profile websites that were hacked included the Malaysian Communication and Multimedia Commission, the Universiti Sains Malaysia and the Public Works Department. The hackers left behind a political message alluding to the disputed Ambalat issue and Malaysia's Ops Tegas. Ops Tegas was a nation-wide law enforcement operation which targeted illegal immigrants.

The report further mentioned that the hacker left the following message on the Public Works Department website:

With respect,

In the name of the law, I order you, Malaysian government, please retreat from Indonesian area. Please don't be too greedy. Indonesia is having bad days recently. The natural disasters, increasing poverty, etc. Your country is much more prosperous than Indonesia. Don't you be ashamed?

FYI. I'm not a hacker.

Re-rationalising Cyber Attacks

The writers of this NTS Alert use the word 'alleged' repeatedly throughout to exercise caution when linking international cyber attacks to conflicts between states, for several reasons. The main reason is that, while ICT has developed rapidly over the last few decades, most states are still ill-equipped in evidence gathering and digital forensics. While there is the technological capability to trace and therefore locate the physical location of cyber attacks, it remains difficult to determine the actual perpetrators and their motives unless they are caught and prosecuted. In the minds of traditional security analysts, cyber vandalism could easily be passed off as acts of terrorism while commercial hacking could be misintepreted as cyber espionage.

In all of the international cyber attacks cited above, news reports, political observers and security specialists were quick to frame and link these cyber attacks to strained diplomatic and international relations and armed conflicts, particularly in the case of Georgia. Despite the lack of actual evidence and in the absence of any arrests, attempts at rationalising cyber conflicts remain speculative at best and politicised at worst. As pointed out by political observer, Ronald Deibert,

'In spite of the alarm, there are no empirical examples of cyber-terrorism to date, unless the term is used so broadly as to encompass politically motivated hacks on websites and occasional inconveniences caused by denial of service attacks.'

Perhaps more worrying is the potential for such speculation and politicisation to intensify already- deteriorating diplomatic relations between affected nations.

Policy Pathways in National Cyber Security Policies

Following the recent spate of international cyber attacks, the issue of cyber security has inevitably received increased attention from the security community. In certain countries, the issue of cyber security has been elevated to the level of high politics and figures prominently in the national security agenda and ICT architecture. Cyber security policies have been formulated with the intent to defend the integrity of states' information systems and communication networks while national cyber security agencies in its different permutations have been created to institutionalise these policies. Most of these cyber security doctrines were articulated within the language of traditional security norms that emphasises state security and sovereignty.

For instance, at the highest international forum and as mentioned earlier, the Secretary-General of the UN's ITU, Dr Toure warned that the next world war may occur in cyberspace. His warning leaves little to the imagination.

In a US government report titled *Cyberspace Policy Review* released in May 2009, it was mentioned that threats to cyberspace have security implications for the global economic and security challenges of the 21st century. Other news reports quoted the Director of US National Intelligence as saying that the biggest cyber threat facing the US is from other nation-states, particularly Russia and China.

In an interview with the British Broadcasting Corporation, the UK prime minister said that terrorists are using the internet in an exploitative way and therefore Britain needs to develop a national security strategy to protect itself from organised crime and terrorist threats from individuals, companies and governments.

Suleyman Anil, a senior official with NATO, was quoted in news reports as saying that 'cyber defence is now mentioned at the highest level along with missile defence and energy security.' In the same report, Anil suggested that rogue nations would resort to cyber terrorism to shut down formal online communication networks and the websites of official institutions.

In Southeast Asia, Singapore and Malaysia have taken a stand on cyber security albeit with slight variations in conceptual models. Prior to the launching of the Singapore Infocomm Technology Security Authority (SITSA) on 1 October 2009, the Ministry of Home Affairs announced that the SITSA mission is to secure the country's information technology environment against external threats to national security such as cyber terrorism and cyber espionage. Amongst its other area of focus, SITSA is also responsible for the country's planning, preparedness and response against major external cyber attacks. Its immediate tasks is twofold: First, it plans to strengthen the critical information infrastructure against cyber attacks and second, to achieve a higher level of national preparedness in response to cyber attacks.

The Malaysian cyber security agency, CyberSecurity Malaysia, was established in 2007 under the pur-

view of the Ministry of Science, Technology and Innovation, to reduce the nation's vulnerability in ICT systems and networks, amongst other objectives. However, CyberSecurity Malaysia is not a law enforcement agency but instead provides cyber forensics and analysis and also provides expert witnesses in court. The agency operates within a larger national cyber security policy framework designed to support a K-economy (knowledge-based economy). Although there was no mention of specific threats such as cyber terrorism, it frames cyber threats as one which is detrimental towards its use of ICT for socio-economic development.

Securitisation of Cyberspace

Judging by the national cyber security policies as highlighted earlier, it appears that cyberspace has effectively been securitised to the extent that states have generally adopted a defensive cyber security posture. Most cyber security policies are framed within the language of national security and in the interests of protecting national economies. States and the business community are increasingly vulnerable to cyber attacks, cyber espionage and commercial hacking. The security threats posed by cyber terrorists from rogue nations and 'hackers' posed significant danger to the social, political and economic survival of nations, as security specialists and policymakers have argued. In fact, if left undeterred, cyber wars could even lead to a third world war, as Dr Toure has warned. Thus, the survival of states and the global economy is dependent on the institutionalisation of a cyber security agenda, which is primarily targeted at securing the integrity of the national communications and information architecture and the protection of classified data.

Humanising Cyberspace

However, there is also the element of human security in cyberspace which must be taken into consideration in analysing the security implications of cyberspace. States are not the only referent object as the widespread implementation of ICT has transformed society into one which is dependent on the production and delivery of information. The general consensus is that ICT was responsible for the transformation from the Industrial Society to the Information Society. Access to information has been a key characteristic of the Information Society. In fact, to a certain extent, vulnerabilities in the Information Society is measured by the degree of an individual or society's acessibility to information.

In his speech which appeared on the *Bangkok Post* news website, Professor Vitit Muntarbhorn outlined several issues which test the linkage between human security and the information age. Amongst these issues are 'access to information and education, reduction of internet gap, cyberspace law and human capacity building for information security and community-based approach'.

Professor Vitit opines that human security is dependent on the access to information and education, and are interlinked with access to quality education, which can be delivered on the ICT platform.

Furthermore, a person's potential for development can be increased if there is access to modern communication channels. Thus computer literacy, which is a basic prerequisite for many jobs, is necessary in the employment market in the Information Society. However, he pointed out that there is a wide internet gap between developed and developing societies which further disadvantages developing communities' economies. The internet gap has to be reduced to decrease this disparity.

The liberalisation of cyberspace serves as a liberating force for human security because people are free to express themselves and communicate via cyberspace. However, state regulations which attempt to control cyberspace may be met with resistance, although it could serve to protect copyright laws and prevent human rights abuses.

Professor Vitit advocates human-capacity building to deter any compromise in information security. Staff who are information-proficient and skilled in computer skills and are of the suitable psychological make-up could respond to the needs of an information security environment better than those who lack these attributes.

Finally, a community-based approach towards the promotion and protection of human security would lead towards the positive use of information. This requires the drawing in of community participation of civil society organisations, community watchdogs as well as the media in generating the right information, which could then be disseminated to the larger society.

Conclusion

The international cyber attacks incidents in recent years have awoken a certain consciousness on the need to extend national security interests to the realm of cyberspace. As if triggered by the international DDoS attacks which occurred in Georgia and then Estonia, followed by the US and South Korea, states which have a highly developed ICT structure have taken the issue of cyber security to the next level. The institutionalisation of cyber security agencies and national cyber security policies marked a turning point in the evolution of international politics, conflicts and warfare.

Amidst these developments, there is also a growing concern amongst non-governmental organisations, global civil society and political observers of the impact of the securitisation of cyberspace on human security. This new development also raises questions about the impact of national cyber security policies on national governments in terms of governance and bureaucratic procedures. Another issue of concern is how would these national cyber security policies affect international cooperation? Would it lead to greater cooperation or to a widened technological or internet gap that would leave developing economies and societies further behind? These are some of the issues that will be discussed in the next edition of the NTS Alert.

EU Convention on Cybercrime

Opening for signature	Entry into force
Place: Budapest Date: 23/11/2001	Conditions: 5 Ratifications including at least 3 member States of the Council of Europe Date : 1/7/2004

Status as of October 14, 2009.

Presently, transnational cooperation on cyber security is certainly not comprehensive enough. To begin with, international cooperation lacks adequate global participation and thus support. It is not as extensive as the global use of ICT. As of 12 October 2009, despite its limitations, the European Union (EU) Convention on Cyber Security is perhaps the most comprehensive and extensive, although the agreement is only signed by EU member states, the US and a handful of others.

Refer to appendix for complete list.

Glossary of Key Cyber Security Terms

Cyberspace	An environment in which digitized information is distributed on networks of computers.
Cyber Security	Measures taken to protect computers or critical infrastructure, although some experts suggest that it is about protecting everything of value.
Cyber Warfare	Using computers and the Internet to attack others via their computer systems. Targets may include military computer networks, power grids, banks, and government and media Web sites. Most often the goal is to disrupt the functioning of the target system.
Cyber Crime	Criminal activities that make use of computers or networks.
Distributed Denial-of-Service Attacks	Flooding the networks or servers of individuals or organizations with false data requests so they are unable to respond to requests from legitimate users.
Cyber Terrorism	The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents.
Cyber Espionage / Cyber Spying	The act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers. Source: wikipedia
Note:	*There is no standard definition of cyber security terms since perception of security threats varies according to context. Therefore, this list is to be treated as a general reference only and not to be cited in relation to the NTS Alert.*

Source: The U.S Federal Bureau of Investigation.Available at <http://www.america.gov/st/peacesec-english/2009/September/20090917175715sjhtrop0.2718012.html>.

References

About us, Cybersecurity Malaysia, Available at <http://www.cybersecurity.my/en/about_us/establishment/main/detail/733/index.html?mytabsmenu=0>.

Bush Orders Guidelines for Cyber-Warfare, Washingtonpost.com, February 7 2003. Available at <http://www.washingtonpost.com/ac2/wp-dyn/A38110-2003Feb6?language=printer>.

Buzan, Barry, Ole Waever and Jaap de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, United Kingdom, 1998.

Cyberspace Policy Review, National Security and Homeland Security Councils, United States Government, May 2009.

Cybercrime versus Cyberlaw, McAfee Virtual Criminology Report, McAfee Inc., 2008.

Cybercrime: The Next Wave, McAfee Virtual Criminology Report, McAfee Inc., 2007.

Unsecured Economies: Protecting Vital Information, McAfee Inc., 2008.

Deibert, Ronald, 'Black Code: Censorship, surveillance, and the militarisation of cyberspace', vol. 32, no. 3, pp. 501-30, *Millennium: Journal of International Studies*, 2003.

European Union Convention on Cybercrime. Available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>.

'Human security as a challenge for the information age', *BangkokPost.com*, 4 September 2009. Available at <http://www.bangkokpost.com/opinion/opinion/23217/human-security-as-a-challenge-for-information-age>.

'ITU chief stresses need for cooperation to protect cyberspace', *United Nations Radio*, 6 October 2009.

Kierkegaard, Sylvia, 'Cracking down on cybercrime global response: The Cybercrime Convention', *International Information Management Association*, vol. 5, issue 1, 2005.

Malaysia's National Cyber Security Policy, Ministry of Science, Technology and Innovation. Available at <http://www.nitc.org.my/index.cfm?&menuid=57>.

'Nato says cyber warfare poses as great a threat as a missile attack', *guardian.co.uk*, 6 March 2008.

Schneier, Bruce, *Cyberwar: Myth or Reality,* November 2007. Available at <http://www.schneier.com/essay-201.html>.

Trends for 2008, Symantec Corporation, Symantec Internet Security Threat Report, 2009. Available at <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiv_04-2009.en-us.pdf>.

Understanding Cybercrime: A Guide for Developing Countries, ITU Telecommunication Development Center, April 2009.

Zubir, Mokhzani, *Exchange of 'cyber-fire' during the Malaysia-Indonesia Ambalat dispute: A lesson for the future*, Centre for Maritime Security and Diplomacy, 2005.

Appendix

Member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra										
Armenia	23/11/2001	12/10/2006	1/2/2007				X			
Austria	23/11/2001									
Azerbaijan	30/6/2008				X	X	X	X		
Belgium	23/11/2001									
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Croatia	23/11/2001	17/10/2002	1/7/2004				X			
Cyprus	23/11/2001	19/1/2005	1/5/2005				X			
Czech Republic	9/2/2005									
Denmark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Finland	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia	1/4/2008									
Germany	23/11/2001	9/3/2009	1/7/2009		X	X	X			
Greece	23/11/2001									
Hungary	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Iceland	30/11/2001	29/1/2007	1/5/2007		X		X			
Ireland	28/2/2002									
Italy	23/11/2001	5/6/2008	1/10/2008				X			
Latvia	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein	17/11/2008									
Lithuania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003									
Malta	17/1/2002									
Moldova	23/11/2001	12/5/2009	1/9/2009			X		X		
Monaco										
Montenegro	7/4/2005			55						
Netherlands	23/11/2001	16/11/2006	1/3/2007				X	X		
Norway	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Poland	23/11/2001									
Portugal	23/11/2001									
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005	14/4/2009	1/8/2009	55			X			
Slovakia	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spain	23/11/2001 r									
Sweden	23/11/2001									
Switzerland	23/11/2001									
Former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Turkey										
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
United Kingdom	23/11/2001									

Compiled, Published and Distributed by NTS-Asia Secretariat, RSIS Centre for NTS Studies, NTU

Non-member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Canada										
Chile										
Costa Rica										
Dominican Republic										
Japan										
Mexico										
Philippines										
South Africa										
United States		29/9/2006	1/1/2007		X	X	X			

Total number of signatures not followed by ratifications:	20
Total number of ratifications/accessions:	26

Notes:
(55) Date of signature by the state union of Serbia and Montenegro.
a: Accession - s: Signature without reservation as to ratification - su: Succession - r: Signature “ad referendum”.
R.: Reservations - D.: Declarations - A.: Authorities - T.: Territorial Application - C.: Communication - O.: Objection.
Source : Treaty Office on http://conventions.coe.int