Email not displaying correctly? Click here to view it in your browser.

CENTRE FOR NON-TRADITIONAL SECURITY STUDIES

INSIGHT

A PUBLICATION OF THE CENTRE FOR NON-TRADITIONAL SECURITY (NTS) STUDIES

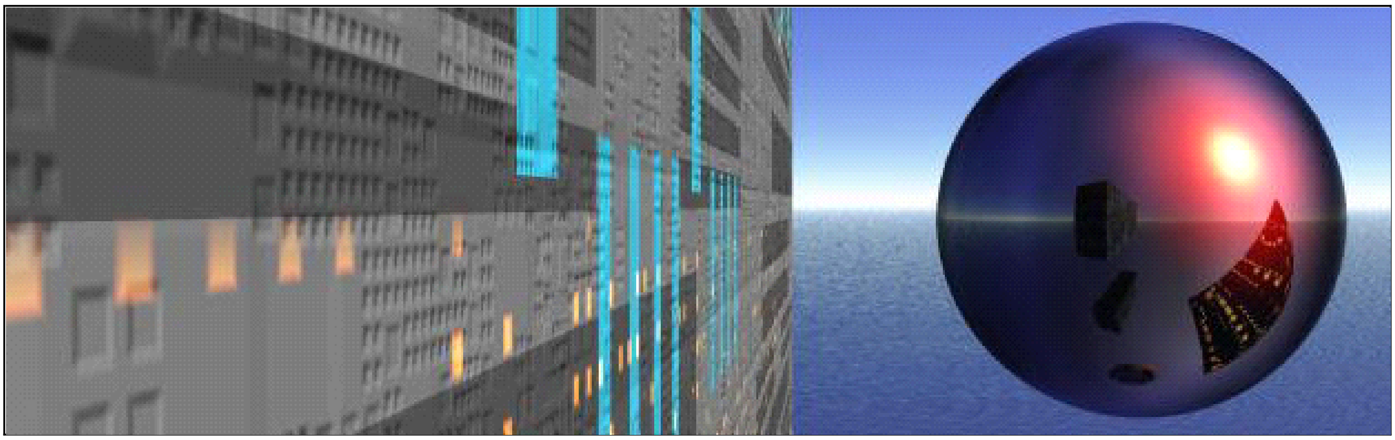
NTS Insight no. IN13-05, July 2013

Click here for the PDF version.

Cyberwarfare: Logged and loaded, but wither Asia?

Cyber operations could have as devastating an impact on populations as conventional military weapons. With militaries already in the process of developing cyberwarfare as a means of battle, there is an urgent need for policymakers to understand this new realm and develop norms and rules to govern it. In this respect, the developing world has lagged behind the developed world. With more and more countries wiring their infrastructure to cyberspace, however, the developing world cannot afford to be left out of the international discussion on cyberwarfare. This NTS Insight discusses how the developing world can build capacity in this area.

By Elina Noor
Guest contributor



Cyberspace is emerging as the perfect extension of, and complement to, warfare for a number of practical reasons, including its cost-effectiveness and the potential for countries and other actors to exploit the legal ambiguities surrounding the notion of cyberwarfare.
Credit: remoran.

Contents:

- **Consortium of NTS Studies in Asia Website**
- **RSIS Centre for NTS Studies Website**

Recommended citation: Elina Noor, 'Cyberwarfare: Logged and loaded but wither Asia?', *NTS Insight*, no. IN13-05 (Singapore: RSIS Centre for Non-Traditional Security (NTS) Studies, 2013).

Introduction

States are increasingly no longer fighting or planning to fight wars the old way. Instead of amassing troops and weapons on a country's borders, the growing penchant – particularly among major powers with technological superiority – is for remote-control wars to be fought from a safe, ensconced distance.

The revolution in military affairs that first delivered the precision-guided heavy weaponry of Operation Desert Storm in 1991 paved the way for the 'virtual war' of Operation Allied Force in 1999. Cruise missiles, which represented 8 per cent of total munitions during Operation Desert Storm, took on an even more significant role in Kosovo in 1999, making up 35 per cent of total munitions.[1] The 'shock and awe' campaign of Operation Iraqi Freedom in 2003 saw that trend continue. The latest iteration of that shift is the US drone attacks in Afghanistan and Pakistan.

These developments are now being layered over by another realm of complexity – cyberspace – that seemingly offers greater cost-benefit advantages to fighting wars but that also poses many questions and challenges to traditional state-centric conceptions of security, legality, sovereignty and territory.

This NTS Insight will begin by explaining how cyberspace alters the cost-benefit equation of warfare and strains traditional concepts of territorial integrity and national sovereignty. The next section will consider whether a state's recourse to cyberwarfare as a new method and means of conflict would and should fall within the existing body of international law (*jus ad bellum*).[2] To conclude, this NTS Insight will call for Asia to play a greater role in the evolving discussion on regulating cyberwarfare, as it risks being sidelined by a dominant few as norms and rules begin to crystallise. In particular, it will urge institutions within Tracks One and Two to initiate or seek participation in creative efforts – with each other, as well as with the private sector, an often overlooked and undervalued component in the larger policy debate on cyberwarfare.

^ To the top

Cyberwarfare as a game changer?

As an emergent military domain additional to air, sea, land and space, cyberspace is turning into the perfect extension of, and complement to, warfare for a number of practical reasons. To put into context, cyberspace is essentially the product of an interconnected network of digital systems and infrastructure spread across the world. The result is a virtual realm that exists parallel to the physical, kinetic world. What is notable about cyberspace is that there are no natural or geographic borders. Instead, it is an undifferentiated landscape of constantly dynamic packets of data routed from one node to another. In this expansive battlefield, attacks can be quick, if not instant. Also, identities – already difficult to verify on the Internet – can be masked through Internet Protocol (IP) spoofing[3] or by complicated routing patterns to preserve stealth and anonymity.

A cyber-attack could disrupt energy supply to households. In the searing heat of summer or the freezing temperatures of winter, this could endanger the lives of particularly vulnerable segments of a nation's population such as the young and the old.

Credit: Jonas in China / flickr.

The use of cyberspace as a means and method of conducting warfare can also be relatively cost-effective, depending on the complexity of the operations executed – an important advantage at a time of budget sequestration and austerity measures. Even at the costlier and more sophisticated end of the scale, Stuxnet, arguably the first malware weaponised and released with intent to destroy critical infrastructure in peacetime, has been estimated to have cost only several million US dollars.[4] With the code discovered and dissected, it will be cheaper to replicate or even improve upon Stuxnet for future attacks.[5] Further, a botnet[6] army can be marshalled at minimal cost with a few strokes of the keyboard and zero movement of logistics. Amassing force can, in fact, be cheap in the digital age. Crucially, in a war-weary era with the media managing to both horrify and desensitise millions to the human costs of war, cyberwarfare risks no 'boots on the ground' or 'coffins draped in flags'.

It is also entirely possible to envisage attacks conducted in cyberspace producing kinetic damage. Stuxnet proved this when it temporarily disabled at least 1,000 of 5,000 centrifuges in the last of a series of attacks on Iran's Natanz plant just a few weeks after the worm was discovered.[7] In modelling tests conducted before Stuxnet was unleashed, the worm managed to reduce to rubble a replica of Iran's P-1 nuclear centrifuge by directing it to slow down and speed up unpredictably. Stuxnet brought the feasibility of physical destruction by way of a cyber-attack one step closer to reality.

The true value of cyberspace as a means and method of warfare, however, lies in its power as a force multiplier to conventional warfare. Not unlike the supplementary role of air power to ground assault (or vice versa, depending on the doctrine subscribed to), cyberwarfare can preface, supplement or augment the kinetic effects of warfare. In extreme scenarios, malware could be delivered to manipulate or disable the operating systems of weaponry, air traffic control or emergency services to exacerbate chaos, injury and destruction caused by missile strikes or firefights.

The point is even more important when one considers how much of a nation's critical infrastructure – from the electricity grid to waste management and power plants – is now connected to, and operated in, cyberspace. Within this context, a single employee with access to an infrastructure's control system could manipulate it for malicious purposes. For example, in Maroochy Shire in Australia in 2000, a discontented employee seized control of a wastewater facility's supervisory control and data acquisition (SCADA) system 46 times using a notebook computer and a radio transmitter. He triggered the spillage of 264,000 gallons of sewage into nearby streams and rivers over two months.[8] Similarly, whole regions of a nation could be plunged into darkness for months simply by remotely disabling a few large transformers of an electricity grid.

The existing legal ambiguities surrounding warfare and conventional armaments are obfuscated further by cyberspace. There is, for example, a plethora of cyber-related terminology mentioned in relation to cyberwarfare – computer network attack/defence/exploitation, information warfare, cyber espionage, cyberterrorism, hacking. What could be confusing is that while some of these activities may be criminal offences, they rarely amount to cyberwarfare. Also, some of these terms sometimes mean the same thing: computer network exploitation and cyber espionage, for example, both describe intelligence and data collection operations through computer systems or networks.

There is in fact no uniform definition of cyberwarfare. The US Department of Defense, for example, refers to the term 'offensive cyberspace operations' as 'cyberspace operations intended to project power by the application of force in or through cyberspace';[9] and while Australia's defence White Papers of 2007 and 2009 have acknowledged cyberwarfare, they have not provided a definition of the term.[10]

Additionally, although the stakeholders of cyberspace comprise both the public and private sectors, the domain is neither owned nor governed by anyone. Also, no body or framework of laws currently regulates its conduct or operations at the global level. There are voluntary laws such as the Council of Europe's Convention on Cybercrime but these do not address the use of cyberspace as a method or means of war, *per se*.[11] Similarly, national laws do not yet tackle cyberwarfare specifically. Even if they did, the lack of harmonisation among these laws and politicisation of the matter would make oversight of the issue a challenge. This, of course, plays to the advantage of strategic ambiguity that cyberwarfare offers.[12] Not only can the anonymity of cyber-attacks offer states the cover of plausible deniability but the lack of an international legal regime governing the conduct of warfare through or in cyberspace means that laws will have to play catch-up to reality.

^ To the top

The legality of cyberwarfare

There is the view that the use of cyberspace on its own can never amount to cyberwar although it can play an auxiliary role in military operations.[13] Moreover, cyber operations through still evolving technologies have until now only caused mass disruption rather than destruction. The argument is that if cyber operations do at all need to be regulated, they would require a new and different legal regime separate from that governing kinetic warfare.

There are four responses to this. First, regardless of whether war is to be understood conventionally as the conduct of hostilities between at least two state parties or whether it is to be more liberally interpreted, the fact remains that nations are developing capabilities to conduct operations in cyberspace amounting to, or in support of, hostilities. They are, in other words, exploiting cyberspace as a means and method of warfare. A 2011 estimate identified 33 states that include cyberwarfare in their military planning and organisation (given the limitations of open-source data, there may actually be more).[14] There is thus an urgent need for a set of regulations to guide and govern the conduct of cyber operations as they are developed and executed.

Nations are already exploiting cyberspace as a means and method of warfare. There is an urgent need for a set of regulations to guide and govern the conduct of cyber operations as they are developed and executed.
Credit: ilco.

Second, a new legal framework drafted especially to govern these cyber operations may quickly be rendered limiting or outdated given the very pace of unfolding technological advancement.

Third, this NTS Insight asserts that kinetic and cyber operations are in fact comparable and attacks in the cyber domain can constitute a *means and method* of war rather than an actual state of war. As a method of warfare executed by the military command of a state, cyber operations should be regulated by a set of norms and/or laws in the same way that other kinetic weapons are. This is particularly since the consequences of cyber operations can potentially be as devastating as kinetic ones.

Fourth, and perhaps most persuasively, is that there is the advantage of an existing analogical corpus of unconventional weapons – nuclear, radiological, biological and chemical – developed during or since World War II that offers insightful guidance on how existing international law may be applied to cyberwarfare. The starting point to this approach is the UN Charter. Articles 2(4) and 51, in particular, determine the legality of a state's recourse to force. The former deals with the 'threat or use of force',[15] and the latter, 'armed attack'.[16]

Although Article 2(4) urges Member States to refrain from the threat or use of force 'against the territorial integrity or political independence of any state', it leaves open the meaning and ambit of 'force'.[17] Even assuming a conservative interpretation of force to mean armed force using a weapon, the International Court of Justice's 1996 advisory opinion on the legality of the use of nuclear weapons bears weight. According to the Court, Articles 2(4), 51 and 42 of the UN Charter 'do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon …'[18] This would seem to tie into the consequences-based interpretation of 'force' where, if the effects of a cyber-attack are as destructive as those of any kinetic attack, the cyber-attack would amount to a use of force.

Where physical destruction is instantly apparent, this would be simple. However, if a cyber-attack disables a country's electricity grid, it is unclear whether such an act could be considered a use of force although it could potentially have devastating knock-on effects to life and property after a prolonged period of time. How far down the chain of causation could damage to life or property be readily attributable to such a cyber-attack? The situation becomes even less clear if a cyber-attack takes out a country's stock exchange, or banking or financial sector. Economic turmoil might not be a kinetic consequence but it could arguably be as devastating as physical destruction to a state and its national sovereignty.

The other concern is that Article 2(4) deals expressly and exclusively with states. This presumes that it would be easy to discover who initiated the cyber-attack when in all likelihood, it would serve the perpetrator best if it is not. For example, although *The New York Times* identified the US and Israel as being behind Stuxnet, neither country has admitted responsibility.[19] Moreover, if citizens of Country A voluntarily launched cyber-attacks against Country B at their government's persuasion over a nationalist dispute, they would not be under the 'effective control'[20] of their government and their actions would not fall within the 'use of force' scope of Article 2(4) of the UN Charter.

Article 51 of the UN Charter, on the other hand, is silent on the perpetrator. However, the explicit mention of 'Member of the United Nations' as victims of an armed attack and their right to self-defence seems to exclude the occupied territories of Palestine and others not yet a member of the organisation for example.

In the absence of an actual incident, the question of whether a cyber-attack that does not result in significant destruction of life and property or one that belatedly causes it would sufficiently constitute an 'armed attack' within Article 51 remains unanswered. Some commentators have suggested that in addition to the qualitative scale and effects of an operation, it is the specific intent of the perpetrating government to violate another state's 'sphere of sovereignty' that would lend to the aggressive intent of an attack.[21] Crucially, the argument goes, this would exclude the accidental spillover effects of malware that spreads beyond its target(s). In a case like Stuxnet, which has made its rounds in several waves to different countries, this would arguably exonerate the parties behind the malware from having conducted an 'armed attack' against any other state beyond Iran.

^ To the top

Conclusion: Where is Asia?

As discussed, there are greater uncertainties than there is clarity on the issue of cyberwarfare in international law. It is to the credit of the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence that it convened a group of independent experts to draft a manual on the international law of cyberwarfare ('Tallinn Manual').[22] Prepared over three years, the effort represents a substantial contribution to clarifying the state of law with regard to cyberwarfare and will likely be used as a starting reference point in international efforts to consolidate this body of law.

However, the debate at large is currently being driven and dominated by only a handful of nations, primarily the US, and to a lesser extent, the UK, Australia and a few European countries. Despite the hype about Asia's rise, Asia is curiously muted if not completely silent on the issue. Yet, the challenges of war in or using cyberspace do not solely affect developed, western or major powers. To be sure, such challenges occupy different levels of priority for various states depending on their level of technological development and interconnectedness as well as their respective domestic political situations. Nevertheless, every country that has its critical infrastructure connected to cyberspace has a stake in this ongoing conversation and how it unfolds.

Currently, it can be seen that norms and rules on cyberwarfare are evolving rapidly to catch up to the phenomenal speed at which related strategic policies and military command structures are being developed. It is absolutely crucial that as many countries as possible – in Asia and the rest of the developing world – participates now when norms are being shaped rather than later when laws have been crystallised and there is little but protestations left to be made. It is in every country's interest to ensure that cyber operations are conducted within a clear and just set of international rules accepted by most, if not all, states for the ultimate purpose of protecting its own people.

Recommendations

Within the noodle bowl of Track One cooperative security mechanisms in Asia such as ASEAN, the ASEAN Regional Forum (ARF), the ASEAN Defence Ministers Meeting (ADMM) and the ADMM Plus, there has been an encouraging increase, reflected in the rhetoric, in the level of awareness of cybersecurity issues. Part of this push has been driven at the Track Two level by institutions such as the Council for Security Cooperation in the Asia Pacific (CSCAP) which published a memorandum on cybersecurity in May 2012 proposing key practical recommendations for the consideration of the ARF.[23] However, while cybersecurity subsumes cyberwarfare, they are not the same thing and special consideration must be given to the latter because of its onus on and implications for the state as the primary arbiter of peace, security and conflict. Further, the current rhetoric on the urgency of cooperation in cyberspace should translate into action.

At the government-to-government level, security and defence cooperation should be expanded to include tabletop exercises and gaming scenarios involving cyberspace to promote greater trust and to build confidence. The concept of interoperability in military affairs should transcend the virtual realm so that there can be seamless cooperation among neighbouring countries (or beyond) in the case of a major cyber-attack on one or more of them. With the infrastructure of cyberspace stretching across borders – through networks of servers located in different countries, fibre optics on the ocean floor, or the cloud – such cooperative exercises should be the norm.

A key component of effective policy solutions will be the engagement of the private sector – often overlooked and treated as a separate entity – in the public policy debate. The public/private dichotomy is especially entrenched in Asian discussions of cyberspace and cybersecurity. As a consequence, the two 'industries' often speak past each other when they are not speaking in entirely different languages altogether. Thus, while there are formidable technical skills to be harnessed from the private sector, there is little understanding or coordination of the policy directions that should drive this operational knowledge in practice, and particularly in the context of cyberwarfare.

If Track One is unable or unwilling to initiate tabletop or simulation exercises either on its own or in collaboration with Track Two and/or the private sector, it would be entirely possible for proactive Track Two institutions to simply reach out to and involve the private sector in policy roundtables. Simulations could also be held at information technology (IT) security conferences around the region to create awareness not only of the technical challenges involved but also the overarching strategic policies needed to guide cyber operations. Such exercises would encourage the public and private sectors to learn from each other and to communicate in a common language.

Track Two institutions and personnel from around Asia could also work with multilateral international organisations such as the International Committee of the Red Cross in exploring and elaborating the sets of rules that should govern the evolution of cyberwarfare. Through roundtables or smaller interactions, Track Two personnel could actively engage with the legal community – including ministries of justice and bar associations, where relevant – of their own countries to discuss the laws that should give recourse to 'force' in cyberspace as well as the rules of engagement that should shape it. A clear national position on these issues would clarify interactions and negotiations at the regional and/or international level.

^ To the top

About the author

Elina Noor is Assistant Director, Foreign Policy and Security Studies, with the Institute of Strategic & International Studies (ISIS) Malaysia. The views expressed here are the author's own.

Notes

1. See, for example: Michael Ignatieff, *Virtual war: Kosovo and beyond (*New York, NY: Picador, 2000); Michael Ignatieff, 'The new American way of war', *The New York Review of Books*, 20 July 2000, http://www.nybooks.com/articles/archives/2000/jul/20/the-new-american-way-of-war/?pagination=false
2. The treatment of international laws of armed conflict (*jus in bello*) as applicable to cyberwarfare would require its own essay and will not be considered here.
3. Internet Protocol (IP) spoofing is a method of hijacking or forging the IP address of a legitimate host for fraudulent purposes. For a technical explanation, see, for example: Matthew Tanase, 'IP spoofing: An introduction', *Symantec*, 11 March 2003, http://www.symantec.com/connect/articles/ip-spoofing-introduction
4. Stuxnet was reportedly 50 times the size of a typical computer worm. David E. Sanger, 'Obama order sped up wave of cyberattacks against Iran', *The New York Times*, 1 June 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0; Robert L. Mitchell, 'After Stuxnet: The new rules of cyberwar', *Computerworld*, 5 November 2012, http://www.computerworld.com/s/article/9233158/After_Stuxnet_The_new_rules_of_cyberwar; Ben Flanagan, 'Former CIA chief speaks out on Iran Stuxnet attack', *The National*, 15 December 2011, http://www.thenational.ae/thenationalconversation/industry-insights/technology/former-cia-chief-speaks-out-on-iran-stuxnet-attack; 'Fmr. CIA head calls Stuxnet virus "good idea"', *60 Minutes*, CBS News, 1 March 2012, http://www.cbsnews.com/8301-18560_162-57388982/fmr-cia-head-calls-stuxnet-virus-good-idea/
5. Sanger, 'Obama order sped up wave of cyberattacks against Iran'.
6. A botnet is a network of compromised devices, control of which has been remotely seized by a command-and-control (C&C) centre, to propagate malicious software ('malware').
7. Sanger, 'Obama order sped up wave of cyberattacks against Iran'.
8. *Supreme Court* of *Queensland r v Boden*, *Vitek 2002*, *CA no. 324* of *2001, DC no. 340* of *2001*.
9. US Joint Chiefs of Staff, *Department of Defense dictionary of military and associated terms* (joint publication 1-02, 8 November 2010; amended through 15 April 2013), 204, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
10. Richard Addiscott, 'The ADF and cyber warfare', *The Interpreter*, 25 October 2012, http://www.lowyinterpreter.org/post/2012/10/25/The-ADF-and-cyber-warfare.aspx
11. Council of Europe, *Convention on Cybercrime* (CETS no. 185, 23 November 2001), http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
12. Martin Libicki describes cyberspace as 'tailor-made for ambiguity'. Martin C. Libicki, 'The strategic uses of ambiguity in cyberspace', *Military and Strategic Affairs* 3, no. 3 (December 2011): 4, http://cdn.www.inss.org.il.reblazecdn.net/upload/%28FILE%291333532281.pdf
13. Thomas Rid, 'Cyber war will not take place', *Journal of Strategic Studies* 35, no. 1 (2012): 5–32, http://dx.doi.org/10.1080/01402390.2011.608939
14. James A. Lewis and Katrina Timlin, 'Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization' (UNIDIR Resources, Geneva: UN Institute for Disarmament Research (UNIDR), 2011), http://www.unidir.org/files/publications/pdfs/cybersecurity-and-

cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

[15] Article 2(4) of the UN Charter states: ‘All Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations’.

[16] Article 51 of the UN Charter states: ‘Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security’.

[17] For a detailed consideration of the interpretation of ‘force’, see: Marco Roscini, ‘World Wide Warfare – Jus ad bellum and the use of cyber force’, *Max Planck Yearbook of United Nations Law, Vol. 14*, ed. A. von Bogdandy and R. Wolfram (Leiden: Martinus Nijhoff Publishers, 2010), 103–6.

[18] International Court of Justice, *Legality of the threat or use of nuclear weapons*, Reports of judgments, advisory opinions and orders, 8 July 1996, http://www.icj-cij.org/docket/files/95/7495.pdf

[19] Sanger, ‘Obama order sped up wave of cyberattacks against Iran’.

[20] The International Court of Justice determined that effective control needed to be had by a government over individuals or groups for it to held legally responsible for their actions. See: International Court of Justice, *Military and paramilitary activities in and against Nicaragua (Nicaragua v United States of America)*, Judgement of 27 June 1986, http://www.icj-cij.org/docket/?sum=367&code=nus&p1=3&p2=3&case=70&k=66&p3=5

[21] Nils Melzer, ‘Cyberwarfare and international law’ (UNIDIR Resources, Geneva: UN Institute for Disarmament Research (UNIDR), 2011), http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

[22] Michael N. Schmitt (ed.), *Tallinn manual on the international law applicable to cyber warfare* (New York, NY: Cambridge University Press, 2013), http://www.ccdcoe.org/249.html

[23] *Ensuring a safer cyber security environment* (Memorandum no. 20, Council for Security Cooperation in the Asia Pacific (CSCAP), May 2012), http://www.cscap.org/uploads/docs/Memorandums/CSCAP%20Memorandum%20No%2020%20--%20Ensuring%20a%20Safer%20Cyber%20Security%20Environmenet.pdf

^ To the top

About the Centre:

The Centre for NTS Studies, based in the S. Rajaratnam School of International Studies (RSIS), was inaugurated by the Association of Southeast Asian Nations (ASEAN) Secretary-General Dr Surin Pitsuwan in May 2008. The Centre maintains research in the fields of Climate Change, Food Security, Energy Security, Health Security, as well as Internal and Cross Border Conflict. It produces policy-relevant analyses aimed at furthering awareness and building capacity to address NTS issues and challenges in the Asia Pacific region and beyond. The Centre also provides a platform for scholars and policymakers within and outside Asia to discuss and analyse NTS issues in the region.

The Centre is the Coordinator of the ASEAN-Canada Research Partnership (2012–2015) supported by the International Development Research Centre (IDRC), Canada. It also serves as the Secretariat of the initiative.

In 2009, the Centre was chosen by the MacArthur Foundation as a lead institution for its three-year Asia Security Initiative (2009–2012), to develop policy research capacity and recommend policies on the critical security challenges facing the Asia-Pacific. It is also a founding member and the Secretariat for the Consortium of Non-Traditional Security (NTS) Studies in Asia (NTS-Asia).

More information on the Centre can be found at www.rsis.edu.sg/nts.