Abstracts

Modern Piracy in the Malacca Straits and the Role of Navies

TAKAI Susumu*

Tankers and cargo vessels that navigate the Malacca Straits often fall prey to sea robbery. In these attacks, the crew is sometimes killed, and cargo or even the vessel itself are stolen. This sea robbery has appeared frequently since Indonesia suffered its economic crisis ten years ago, and is called modern piracy. Some of the attacks are related to international crime syndicates that can get cargo information from various sources as well as sell cargo and vessels to their clients.

Piracy under the law of the sea means a robbery on the high seas; however, modern pirates do their deeds within territorial waters near the Malacca Straits. For this reason, no State but those with coastline facing the Malacca Straits can punish or arrest these modern pirates. However, even when modern pirates are arrested, they are soon set free, for the coastal States have no article on piracy in their criminal law.

This short article examines the reality of modern piracy in and around the Malacca Straits, and the naval operations to suppress it by the Malaysian and Indonesian navies. Lastly, international cooperation on suppressing modern piracy, such as setting up a piracy information center and introducing a ship location system, is discussed.

* Director, Library, NIDS

Cyber Attack and Legal Regulations

HASHIMOTO Yasuaki*

Since our modern society has come to increasingly depend on computers and their networks due to rapid advances in computer performance and expansion of international networks such as the Internet, cyber attacks have become a non-avoidable crisis. The acts defined by the term, "cyber attack," vary from a simple breach of a system performes by an individual out of mischief, to a large-scale "invasion" in which one State has aggressive intentions against an other State or States. However, a defining characteristic of a cyber attack is that, whether such an attack is carried out by an individual or a nation, it can result in the same amount and degree of damage done to society. This damage may cause the functional disorder of social infrastructure or military related systems, and can have a broad influence on areas as diverse as our civic life and national/international security.

Because a cyber attack by a State is not performed by means of direct, physical destruction using arms, it might not be considered included in the concept of armed attack under international law. However, considering that there may be no substantial difference in the amount of damage than that done by actual military power, the interpretation should be broadened to include cyber attacks within the concept of armed attack. Through such a broader interpretation, a response by the State to a cyber-attack on the basis of the right to self-defence can be legitimized.

Fundamentally if cyber attacks are perpetrated by individuals and terrorists, they should be treated as crimes, and if carried out by a State, as armed attacks. However, because it is difficult to ascertain immediately the identity of an aggressor/attacker and the intention of the attack, we should prepare for adequate responses to either a crime or an armed attack. After the situation becomes clear, it is desirable to shift to the more suitable response system. Further, it might be possible to respond to cyber attacks internationally using multilateral measures based upon the concept of

* Senior Research Fellow, 2nd Research Office, 1st Research Department, NIDS

collective security, since such attacks may be interpreted as a threat to or destruction of international peace and security as a whole. For that purpose, collaboration among the organs concerned, including both crime control and defence organizations, is required. Also, since damage may result to both public social infrastructure and private entities, close cooperation between the public and private sectors is also indispensable. Moreover, in order to cope with cyber attacks effectively, such cooperation must extend beyond the borders of a single country to have an international reach. Japan must take the above-mentioned measures domestically and internationally to enable not only countermeasure technologies for cyber attacks but also legal regulations related to cyber attacks to be more effectively established.

Nuclear Weapons in South Asia

IZUYAMA Marie[*]
OGAWA Shin'ichi[**]

Government and people in Japan raised vocal criticism against South Asia's nuclear tests in 1998. However, debate in Japan rarely go beyond a principled position, that is, "How to bringing India and Pakistan into the NPT and CTBT?" Departing from this conventional position, this article aims to grasp the strategic implications of the tests. It assesses the variables that have influenced the nuclear development of India and Pakistan. It also explores the nuclear and disarmament policies of both States. The authors suggest desirable paths for South Asia's nuclear policy in terms of our national security interests and international peace and stability.

The history of the nuclear programmes of India and Pakistan is reviewed in the first part of the article. India has not pursued its nuclear programme with a single, static motive. Rather, it has developed cumulatively while responding to the external

[*] Senior Research Fellow, 2nd Research Office, 2nd Research Department, NIDS
[**] Senior Research Fellow, 1st Research Department, NIDS

environment, such as China's nuclear test, Pakistan's nuclear development, and the conclusion of the CTBT negotiations. Pakistan's nuclear programme, which clearly targets India, has not been effectively constrained by US non-proliferation policy because of its role in the Afghan war in the 1980s.

In the second part of the article, the nuclear postures of India and Pakistan are analyzed. India's nuclear doctrine is a compromise between "recessed deterrence," "maximum deterrence," and a middle path. The real challenges for India are whether it can develop the capability to deter China, whether to develop SLBM, and how to attain strategic stability vis-à-vis Pakistan. The immediate challenge for Pakistan is to ensure the survivability of its nuclear assets against an Indian strike.

In the third part of the article, the attitudes of India and Pakistan toward the NPT, CTBT and FMCT are explored. After the May 1998 tests, India promised not to hinder the entry into force of the CTBT. This change of policy could possibly create the opportunity for the simultaneous signing of the CTBT by India and Pakistan. Both States would not be positive to FMCT negotiation, as Pakistan would try to catch up with India's stockpile, and India would do the same in relation to China.

In the concluding section, the implications of South Asian nuclear issues for international security are discussed. In order to maintain the norm of "nuclear taboo," the nuclear use by India and Pakistan must be avoided. It is necessary to stabilize the balance of conventional forces, ensure the survivability of the nuclear arsenals of the two countries, and develop effective C3I systems, including an early warning system. However, in the longer term, achieving "nuclear peace" in South Asia may not be compatible with global security. This is because, learning from the South Asian experience, other sets of non- nuclear weapons-states in adversarial relationships could emulate the two and withdraw from the NPT to go nuclear. We should pursue a way to stabilize Indo-Pakistani nuclear relations, thus avoiding the further development of their nuclear capability.

The Economic Security and Arms Transfer Policy of the United States: DTSI and Defense Cooperation with Allies

SATO Heigo*

The Defense Trade Security Initiative (DTSI) was initiated in May 2000 in order to reorganize U.S. export control policy and adjust it to the post-Cold War security and domestic environment. Also, it was partly aimed at dealing with issues such as the globalization of defense industry production and the increased proliferation of military technologies and dual-use technologies.

The major policy goal of the DTSI was to relax export control, and it also sought to: improve inter-operability in joint combat operations with allied countries; standardize the capability gap between the U.S. forces and NATO allies; and maintain the competitiveness of the U.S. defense industry base. The United States aimed to expand defense industry cooperation with allied countries and form a community of joint technology through 17 separate but interrelated initiatives. The DTSI consists of four clusters of initiatives. Those are: commercial export and related initiatives; transformation of license applications and related initiatives; relaxation of International Traffic in Arms Regulations (ITAR application to allied countries); and government approved transfers of military goods and related technologies. The Clinton and George W. Bush administrations promoted these initiatives in both domestic export control reorganization and cooperation among allies through the DTSI, beginning with Great Britain and Australia.

However, there are criticisms of the implementation of the DTSI. The U.S. Congress criticizes it as weakening the influence of Congress over arms transfer. Second, standardization of export control with European countries may weaken the export control of the United States, since Europeans have lax control compared to the U.S. Third, if the DTSI is fully implemented, the European countries will have to

* Senior Research Fellow, 1st Research Office, 2nd Research Department, NIDS

purchase U.S. weaponry to establish interoperability with the United States. Therefore, it is said that the DTSI is merely an export promotion measure for export promotion for the United States. Fourth, the DTSI assumes that export control is no longer a viable measure to curb weapons proliferation, so that promoting the DTSI may end in emphasizing counter-proliferation measures including military operations, rather than undertaking a strict application of existing export control mechanisms.

Japan must seriously consider restructuring her domestic restraints on arms transfers if she wishes to take part in these initiatives.

Islamic Extremism and Russian Defence Policy

SAKAGUCHI Yoshiaki*

Throughout the 1990's, Russia has considered Islamic extremism a serious threat to its national security due to the separatist movement in Chechnya, one of Russia's regions in the northern Caucasus. It sees the movement as connected with Islamic extremism and as radicalized. Since the summer of 1999, many Russian people have been killed by terrorist bombings in Moscow and other cities of southern Russia. The Russian government believes that extremist Chechen guerrillas are the criminals conducting terrorist bombings targeting Russian people, and that the Chechen guerrillas are supported by Osama bin Laden and his terrorist organization, "Al-Qaeda."

The Putin administration gives high priority to defence policy to how to deal effectively with the threat of Islamic extremism from the Caucasian and Central Asian regions. Through the first Chechen conflict from 1994 to 1996 and the second Chechen conflict since 1999, the military leadership has understood that one of the most serious problems facing the Russian military was the low combat ability of its ground forces and the weakness of conventional weapons. Taking this problem into consid-

* Chief, 2nd Research Office, 2nd Research Department, NIDS

eration, President Putin and Defence Minister Ivanov are grappling with military reform, focusing on the improvement of the combat ability of the ground forces and the renewal of conventional weapons. As Putin and Ivanov consider a military posture for dealing with the threat of Islamic extremism in the south as very important, Russian military forces in the Far Eastern Region will be reduced in the near future, reflecting the lack of a serious threat in this region now.