The Importance of Intelligence in the Maritime Domain

Dr. Peter Roell

September 2014

Abstract

In his article the author focuses on maritime terrorism, piracy and armed robbery and energy security in the maritime domain. At the end of his analysis he gives some recommendations for decision makers in politics, in the armed forces, and in the business and public sectors, for potential threats in the maritime domain as well as in the field of economic and industrial espionage.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is objective and task oriented and is above party politics.

In an ever more complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, bringing major opportunities but also risks, decision-makers in enterprises and politics depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, economy, international relations, and security/ defense. ISPSW network experts have worked – in some cases for decades – in executive positions and possess a wide range of experience in their respective specialist areas.

ANALYSIS

Introduction

At the beginning of my article *The Importance of Intelligence in the Maritime Domain* for this year's edition of the publication "Forte de Copacabana", I would like to give two definitions regarding "intelligence" and "maritime domain".

"Intelligence" is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.[1]

"Maritime domain" defines "all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime related activities, infrastructure, people, cargo, and vessels and other conveyances".[2]

In the maritime domain we are facing several threats: maritime terrorism, piracy and armed robbery, territorial disputes in the regional seas, trafficking of illicit narcotics, trafficking of weapons, human trafficking, environmental degradation, global climate change, just to mention a few.

In my contribution I will focus on maritime terrorism, piracy and armed robbery and energy security in the maritime domain. At the end of my article I will give some recommendations for decision makers in politics, in the armed forces, and in the business and public sectors, for potential threats in the maritime domain as well as in the field of economic and industrial espionage.

Maritime Terrorism

Looking at the problem of maritime terrorism I would like to remind you of some incidents:

October 2000

A successful attack was carried out against the U.S. destroyer USS *Cole* in Yemen. 17 U.S. sailors were killed, 39 wounded.[3]

October 2002

The French oil tanker *Limburg* was attacked off Ash Shahir by a terrorist group with connections to Al Qaida. One member of the crew was killed and 90,000 tons of oil spilled into the Gulf of Aden. The monthly container

[1] U.S. Department of Homeland Security, National Plan for Maritime Security: National Plan to Achieve Maritime Domain Awareness, October 2005, http://www.dhs.gov/national-plan-achieve-maritime-domain-awareness [accessed July 1, 2014].
[2] Joseph Milligan, "Maritime Domain Awareness," (presented at the USCG/CREATE Maritime Risk Symposium, University of Southern California, Los Angeles, November 16-18, 2010).
[3] "Attack on the USS Cole," *al-bab.com*, http://www.al-bab.com/yemen/cole1.htm [accessed July 1, 2014].
See also: Raphael Perl, Ronald ORourke, „Terrorist Attack on USS *Cole*: Background and Issues for Congress," The Navy Department Library, CRS Report for Congress, January 30, 2001, http://www.history.navy.mil/library/online/usscole_crsreport.htm [accessed July 1, 2014].

traffic in Yemen shrank from 43,000 to 3,000. The economy of the country declined by one per cent of its GDP and 3,000 dockworkers lost their jobs.[4]

November 2002

Arrest of al-Qaeda's chief planner for maritime terrorism, Abd Al Rahman Al Nashiri, also known as the "Prince of the Sea", in the United Arab Emirates.[5]

Nashiri had developed a strategy including the following four elements:

- Ramming or blowing up medium-sized ships in the vicinity of other ships or in harbours;
- Attacking super tankers from the air with small planes, laden with explosives;
- Underwater attacks against ships using divers;
- Attacks against cruise liners and taking hostages.

August 2003

The arrest in Thailand of "Hambali" – real name Riduan Isamuddin – on August 11, 2003 accused of masterminding the attack on a nightclub on the Indonesian island Bali killing 202 people in 2002, was a great success. This joint operation by Thai and U.S. Intelligence and the arrest of the "Prince of the Sea" underlines the importance of good intelligence.[6]

February 2004

The Abu Sayyaf Group attacked a ferry in the Philippines, 116 people lost their lives.[7]

August 2005

Israel's security service Shin Bet warned four Israeli cruise liners – on their passage to Turkey – about a possible terror attack and redirected the ships to Cyprus.[8]

July 2010

A suicide attack was carried out by the Abdullah Azzam Brigade against the Japanese oil tanker *M. Star* in the Strait of Hormuz, a militant group with connections to al-Qaeda. One member of the crew was injured and the hull severely damaged.[9]

These cases underline the threat situation and the importance of intelligence in the maritime domain. They also demonstrate the serious consequences a lack of intelligence can have. In my research about the Abdullah

[4] "Yemen says tanker blast was terrorism," *BBC News World Edition*, October 16, 2002, http://news.bbc.co.uk/2/hi/middle_east/2334865.stm [accessed July 1, 2014].
[5] Wikipedia, http://en.wikipedia.org/wiki/Abd_al-Rahim_al-Nashiri [accessed July 1, 2014].
[6] Wikipedia, http://en.wikipedia.org/wiki/Riduan_Isamuddin [accessed July 1, 2014].
[7] Wikipedia, http://en.wikipedia.org/wiki/Abu_Sayyaf [accessed July 1, 2014].
[8] Christine Lagorio, "Israeli Cruise Attack Plot Exposed," *CBSNews.com*, August 11, 2005, http://www.cbsnews.com/news/israeli-cruise-attack-plot-exposed/ [accessed July 1, 2014].
[9] Wikipedia, http://en.wikipedia.org/wiki/Abdullah_Azzam_Brigades [accessed July 1, 2014].

Azzam Brigade, however, I found out that Open-Source Intelligence (OSINT) regarding the capabilities and intentions of this group is quite limited.

Piracy and Armed Robbery

Let me turn now to piracy and armed robbery. In this field a lot of open-source information can be found: Reports by the International Maritime Bureau (IMB), reports by police and by security services, studies by think tanks all over the world, insurance companies, banks, shipping companies, media etc.

In its annual report of January 2014 on piracy and armed robbery against ships the IMB reported 79 incidents around Africa in 2013. Of these, 15 were attributed to Somali pirates and occurred near Somalia and the Horn of Africa, down from a total of 75 Somali piracy-attributed attacks in 2012 and 237 in 2011.[10]

The IMB attributes this significant drop in the frequency and range of attacks by Somali pirates to actions by international navies, as well as preventive measures by merchant vessels, including the deployment of privately contracted armed security personnel.

Looking at the West-African coast, attacks against ships are on the rise because adequate naval forces are not available, armed security guards on ships are not present and ‘best practices’ are not observed. For example, Nigeria does not permit armed private security guards on ships. So we can conclude that in combating piracy and armed robbery the presence of navies and private security forces on ships are necessary and showed remarkable results.

In the Gulf of Guinea a worrying trend in the kidnapping of crews from vessels well outside the coastal territorial limits can be observed. Nigerian pirates and armed robbers accounted for 31 of the region’s 51 attacks, taking 49 people hostage and kidnapping 36, more than in any year since 2008.[11] The upsurge of piracy in Nigeria may also be connected to the theft of large quantities of crude oil from pipelines in the Niger Delta.[12]

Regarding Indonesia the IMB reports a high number of “low level opportunistic thefts” in Indonesian anchorages and waters, a rise of armed robbery from 46 in 2011 to 106 in 2013.[13]

[10] ICC Commercial Crime Services, “Somali pirate clampdown caused drop in global piracy, IMB reveals,” January 15, 2014, http://www.icc-ccs.org/news/904-somali-pirate-clampdown-caused-drop-in-global-piracy-imb-reveals [accessed July 1, 2014].
See also: Dr. Peter Roell, “Combating Piracy and Maritime Terrorism – A Common Challenge for Europe and Asia,” International Relations and Security Network (ISN), Center for Security Studies (CSS), ETH Zurich, April 2013, http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=163375

[11] Ibid.

[12] Steven Beardsley, „For a different African piracy problem, Navy seeks solutions on shore,” *Stars and Stripes*, January 21, 2014, http://www.stripes.com/news/for-a-different-african-piracy-problem-navy-seeks-solutions-on-shore-1.262649 [accessed July 1, 2014].
See also: Dirk Steffen, “Troubled Waters? The Use of Nigerian Navy and Police in Private Maritime Security Roles,” ISN ETH Zurich, July 18, 2014, http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=181585 [accessed July 19, 2014].
See also: Cristina Barrios, “Fighting piracy in the Gulf of Guinea Offshore and onshore,” *Brief Issue 20/2013*, European Union Institute for Security Studies (EUISS), Paris, May 2013, www.iss.europa.eu/uploads/media/Brief_20.pdf [accessed July 1, 2014].

[13] “Piracy and Armed Robbery Against Ships, Report for the Period 1 January - 31 December 2013,” ICC International Maritime Bureau, London, January 2014.

But with all these figures we should be careful. It is well known that ship owners are very reluctant to report actual or attempted attacks to the IMB Reporting Center because they want to avoid additional costs and unwanted delays while an incident is investigated.

A spectacular incident occurred in January 2014 when the MT *Kerala* was hijacked in Angolan waters, sailed northwest for more than a week, covering 1,300 nautical miles, during which time three ship-to-ship transfers of the diesel oil cargo were completed, removing 12,270 tonnes. The ship was then abandoned off the coast of Ghana.[14]

The complex nature of the operation indicates a high level of organisation and planning, as well as the intelligence to deliberately target a vessel more than 1,300 nautical miles away and to select it from more than 30 vessels in the area at the time.

The hijacking of a tanker on 22 April 2014 was a clear sign of the continued threat of piracy in the Straits of Malacca despite multinational sea and air patrols. The attack on the tanker MT *Naniwa Maru 1* happened off Port Klang in Malaysian territorial waters. At approximately 0055 local time on 22 April 2014, two vessels – one flying a Mongolian flag – came alongside the ship, which was laden with 4,344 metric tons of marine diesel oil and was sailing from Singapore to Yangon, Myanmar.[15]

The tanker was boarded and five people entered the bridge. The crew of 18 Indonesian, Indian and Thai nationals was held while 2,500 tons of fuel was siphoned off. The robbers departed with three hostages: the master, chief officer and chief engineer.[16]

The theft of oil products from vessels transiting the Strait of Malacca has become more common, perhaps inspired by pirates off West Africa.

All these cases I have described underline – also in the field of piracy and armed robbery – the threat situation and the importance of intelligence. In this context I would like to point out that Open-Source Intelligence (OSINT) should be complemented by reliable secret information.

I also would like to say a few words about an important political, economic and military player, the People's Republic of China and its intelligence services. I am sure that also after the establishment of China's new leadership, the Chinese intelligence services will play an indispensable role in guaranteeing China's internal and external security, which includes intelligence collection in the maritime domain.

Looking at China's primary objectives, the PRC wants

[14] James Bridger, "Piracy in the Gulf of Guinea: Oil Soaked Pirates," *USNI News*, March 10, 2014, http://news.usni.org/2014/03/10/piracy-gulf-guinea-oil-soaked-pirates [accessed July 1, 2014].
[15] Maritime Bulletin: Naniwa Maru No.1 pirates attack – Update from ReCAAP, April 24, 2014, http://www.news.odin.tc/index.php?page=view/article/1398/Naniwa-Maru-No1-pirates-attack--Update-from-ReCAAP [accessed July 1, 2014].
[16] Ibid.
See also: IISS Strategic Comments, "Enduring threat of global piracy," May 2, 2014, http://www.iiss.org/en/publications/strategic%20comments/sections/2014-a6f5/enduring-threat-of-global-piracy-0fb0 [accessed July 1, 2014].
Regarding maritime security see also: Lutz Feldt, Dr. Peter Roell, Ralph D. Thiele, "Maritime Security – Perspectives for a Comprehensive Approach," International Relations and Security Network (ISN), Center for Security Studies (CSS), ETH Zurich, April 2013, http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=162756 [accessed July 24, 2014].

- to become the leading economic world power by 2020, maintaining an economic growth rate of approximately 7%;[17]
- to re-establish its geostrategic importance;
- to increase R&D-investment: from 1.3% GDP to 2.5% GDP by 2020;[18]
- to establish an "economic and technological army" to develop China;
- education and know-how – the key to China's rise.

Although the international media are focusing on the Snowden case and the NSA since June of last year, most foreign intelligence activity against Germany is carried out by the services of the Russian Federation and the People's Republic of China.[19]

According to information released by the Federal Ministry of the Interior in its 2013 Annual Report on the Protection of the Constitution, two Chinese intelligence services are still very active in Germany: the Ministry of State Security – MSS and the Military Intelligence Department – MID. But we have also to mention the Electronic Interception Department of the PLA. Regarding the structures and missions of Chinese intelligence services the 2013 Annual Report states the following:

MSS – Ministry of State Security

The scope of the intelligence missions conducted by the non-military MSS is quite comprehensive. Its personnel resources operating worldwide are considerable. Domestically, the MSS exercises police powers. But the service also plays a central role in external intelligence collection. In Germany, the service is collecting information in the fields of economy and politics. Also, the MSS is gathering information on opposition movements and attempting to suppress their activities.[20]

MID – Military Intelligence Department
Second Department (Er Bu) of the PLA

As integral part of the People's Liberation Army, the MID is a worldwide and proactively operating intelligence service. The service is responsible for collecting information relevant to China's internal and external security and its military potential. Its main intelligence targets are, among others, equipment, structure and potentials of foreign military forces. Other major targets lie in the areas of politics, science and technology.[21]

[17] The World Bank, „China Overview," http://www.worldbank.org/en/country/china/overview [accessed July 1, 2014].
[18] James Wilsdon and James Keeley, „China: The next science superpower?," *The Atlas of Ideas: Mapping the new geography of science*, DEMOS, January 7, 2007, http://www.demos.co.uk/publications/atlaschina [accessed July 1, 2014].
See also: "Research in China: Quantity on schedule, quality catching up," Press Release, DECHEMA e.V., February 2013, www.dechema.de [accessed July 1, 2014].
[19] Federal Ministry of the Interior, 2013 Annual Report on the Protection of the Constitution: Facts and Trends, p. 31, Cologne, June 2014, http://www.verfassungsschutz.de/en/download-manager/_annual-report-2013-summary.pdf [accessed July 1, 2014].
[20] Federal Ministry of the Interior, 2013 Annual Report on the Protection of the Constitution, p. 324, Cologne, June 2014, http://www.verfassungsschutz.de/de/download-manager/_vsbericht-2013.pdf [accessed July 1, 2014].
[21] Ibid.
Regarding Chinese military and security developments involving the People's Republic of China to 2014 see: Annual Report to Congress, Office of the Secretary of Defense, http://www.defense.gov/pubs/ [accessed July 19, 2014].
Regarding China's cyber activities see: Mandiant Intelligence Center Report, APT 1: Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/ [accessed July 1, 2014].

It is well known that the United States is a major target for Chinese industrial espionage, because it is a leader in technology development, particularly in military hardware desired by China's expanding military, and a potential adversary at the forefront of Chinese defense thinking. China has managed to gather a great deal of information on U.S. stealth technology, naval propulsion systems, electronic warfare systems and nuclear weapons.[22]

On May 19, 2014 the United States Department of Justice indicted five Chinese military officers with stealing data from six U.S. companies and unions. Attorney General Eric H. Holder, Jr. announced that the United States for the first time would seek to bring officials of a foreign government to the U.S. to face charges of infiltrating American computer networks to steal data beneficial to U.S. trade competitors and the Justice Department even went so far as to print "wanted" posters.[23]

No wonder that the Chinese government rebuked the United States over its claims of cyber-spying by five Chinese military officers. "The Chinese government, the Chinese military and their relevant personell have never engaged or participated in cyber theft of trade secrets", Foreign Ministry Spokesman Qin Gang said in a statement "The U.S. accusation against Chinese personnel is purely ungrounded and absurd".[24]

From a reliable source I have learned that Chinese hackers have been capable of infiltrating computers of one of the leading U.S. companies in the defense industry – undetected for three years.

Electronic Interception Department (San Bu) of the PLA

While not part of the MID, the Third Departement of the PLA is another intelligence organization providing Signal~~s~~ Intelligence (SIGINT). It is actually the third largest SIGINT operation in the world, after those of the United States and Russia, monitoring diplomatic, military and international communications.[25]

Coming back to Germany, in the field of economic espionage the Chinese intelligence services are focusing on the acquisition of sensitive information concerning new research results or cutting-edge technologies. Due to the intricate and obscure links between the state and private business sector, it is quite difficult to distinguish whether these attempted intelligence-gathering activities by the Chinese are state-driven economic espionage operations, competitive business intelligence activities carried out by private companies or the initiative of individuals.[26]

In his publication of January 2014, *China's Growing Spy Threat*, Maxim Worcester discusses the extent to which Chinese intelligence services are involved in corporate espionage. While the current public debate focuses on the U.S. National Security Agency (NSA), Worcester argues that private companies should spend more time and

[22] Alex Newman, "China's Growing Spy Threat," *The Diplomat*, September 19, 2011, http://thediplomat.com/2011/09/chinas-growing-spy-threat/ [accessed July 1, 2014].
[23] Spencer Ackerman and Jonathan Kaiman, "Chinese military officials charged with stealing US data as tensions escalate," *theguardian*, May 20, 2014, http://www.theguardian.com/technology/2014/may/19/us-chinese-military-officials-cyber-espionage [accessed July 18, 2014].
[24] Timothy M. Phelps, Julie Makinen, "China blasts 'absurd' U.S. charges of cyberespionage," *LA Times*, May 19, 2014, http://www.latimes.com/nation/nationnow/la-na-nn-china-cyber-spying-20140519-story.html [accessed July 18, 2014].
For more information on China's cyber espionage see: Mandiant APT1 Report: Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/
[25] Chinese Intelligence Services, http://www.fas.org/irp/world/china/ [accessed July 1, 2014].
See also: http://www.project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf
[26] Federal Ministry of the Interior, 2012 Annual Report on the Protection of the Constitution, Cologne, September 2013, p. 393, http://www.verfassungsschutz.de/de/download-manager/_vsbericht-2012.pdf [accessed July 1, 2014].

resources in order to protect themselves from Chinese corporate espionage activities. He also provides specific advice on how private companies can recognize and avert attempts to steal data.[27]

When it comes to the maritime domain, I would like to refer to China's expanding drone program for security and economic reasons. The UAVs are useful for patrolling the East and South China Seas, allowing Beijing to maintain a presence in the disputed waters, and play a role in China's anti-access and area-denial strategy.[28]

Beijing has plans to build 11 coastal drone bases by 2015 to increase its abiliy to survey the region for possible intrusions or potential threats.[29]

The U.S. in particular is developing maritime drones for missions that will include intelligence gathering, reconnaissance and surveillance. Under development are Large Diameter Unmaned Underwater Vehicles and the Persistent Littoral Undersea Surveillance System which includes deep and shallow water "gliders" to increase awareness of the underwater battle space.[30]

During the 13th IISS Shangri-La Dialogue 2014, convened in Singapore from May 30 – June 1, U.S. Secretary of Defense, Chuck Hagel mentioned in his speech, that the U.S. will continue to help nations build their humanitarian and disaster reflief capabilities, and upgrade their militaries. For the first time Indonesia will receive Apache helicopters to conduct counter-piracy operations, and control the free flow of shipping through the Straits of Malacca. Furthermore Washington will provide robust assistance to the Phillipines' armed forces, to strengthen their maritime and aviation capabilities.[31]

South Korea will receive "Global Hawk Drones", which will dramatically enhance its intelligence, surveillance and reconnaissance capabilities. South Korea also intends to aquire the F-35 Joint Strike Fighter. In Japan the United States will deploy two additional ballistic missile defense ships and has deployed its most advanced capabilities – including two Global Hawks at Misawa, F-22 fighter aircraft at Kaneda, and MV-22 Ospreys on Okinawa.[32]

Next year the U.S. Navy will introduce the Joint High Speed Vessel in the Pacific and an additional submarine forward station in Guam. As many as four Littoral Combat Ships will be deployed there by 2017. By 2018, the navy's advanced multi-mission Zumwalt-class destroyer will begin operating out of the Pacific. And by 2020, the U.S. want to achieve its target of operating 60% of both its navy and air force fleets out of the Pacific and also

[27] Maxim Worcester, "China's Growing Spy Threat," International Security Network (ISN), ETH Zurich, January 2014, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=176358 [accessed July 1, 2014].
[28] "First Chinese „stealth" drone ‚ready' for test flight," *Asitimes*, May 12, 2013, http://asitimes.blogspot.de/2013/05/first-chinese-stealth-drone-ready-for.html [accessed July 1, 2014].
See also: Christopher Bodeen, "China's Drone Program Appears To Be Moving Into Overdrive," *TheWorldPost*, March 5, 2013, http://www.huffingtonpost.com/2013/05/03/china-drone-program_n_3207392.html [accessed July 1, 2014].
See also: Ian M. Easton and L.C. Russell Hsiao, "The Chinese People's Liberation Army's Unmanned Aerial Vehicle Project: Organizational Capacities and Operational Capabilities," http://www.project2049.net/documents/uav_easton_hsiao.pdf
[29] Jonathan Kaiman and Justin McCurry, "Japan and China step up drone race as tension builds over disputed islands," *The Guardian*, January 9, 2013, http://www.theguardian.com/world/2013/jan/08/china-japan-drone-race [accessed July 1, 2014].
See also: Stephan Blancke, "China – The drone and the cyber space. A reading between the lines," *Counterintelligence*, August 16, 2013, http://stephanblancke.blogspot.de/2013/08/china-drone-and-cyber-space-reading.html [accessed July 19, 2014].
[30] Mark Valencia, "Intelligence Gathering, the South China Sea, and the Law of the Sea," Nautilus Institute for Security and Sustainability, August 30, 2011, http://nautilus.org/napsnet/napsnet-policy-forum/intelligence-gathering-the-south-china-sea-and-the-law-of-the-sea/#axzz37ofQyboW [accessed July 18, 2014].
[31] U.S. Department of Defense, Defense Secretary Hagel's Remarks to Shangri-La Dialogue, Singapore, May 31, 2014, IIP Digital, U.S. Department of State, http://iipdigital.usembassy.gov/st/english/texttrans/2014/05/20140531300639.html#axzz38CcbqpAe [accessed July 23, 2014].
[32] Ibid, p. 8.

they will fly the Hawkeye early warning and unmanned Triton ISR aircraft in the region.[33] These are clear indications that the U.S. is a Pacific power and will be a Pacific power.

Maritime Energy Security

Regarding the subject of Maritime Energy Security I would like to quote Hillary Rodham Clinton speaking on the campus of Georgetown University in Washington on October 18, 2012. In her speech the then U.S. Secretary of State remarked that energy will be a growing priority in U.S. foreign policy of the 21st century for three reasons:

1. Energy is at the "core of geopolitics";
2. Energy is "essential to how we will power our economy and manage our environment in the 21st century" and
3. "Energy is key to economic development and political stability."[34]

Indeed, energy is essential to a nation's security, economic stability, and global trade but it is also particularly vulnerable to attacks and disruption in the maritime environment. Protecting the 11,000 oil and chemical tankers and approximately 1,500 gas tankers, among other vessels that are part of the world merchant fleet, is **the** maritime energy security challenge.[35]

The amount of energy that travels by water is remarkable and highlights why global energy markets are affected by maritime crime. Oil and natural gas from the Persian Gulf provides 40% of global supply, with 15.5 million barrels of oil a day, or 40% of all traded oil, transiting to the Strait of Hormuz. Vessels carrying more than half of the world's oil pass through Southeast Asian waters.[36]

China is the world's second largest oil consumer and the largest oil importer. Oil consumption is expected to grow in China by 5.8% annually until 2015. Oil imported from the Gulf States and Africa comprises 70% of total Chinese oil imports, and remains China's most critical source of energy apart from domestic coal production.[37]

The critical Sea Lines of Communication (SLOCs) that connect China to the Middle Eastern oil-producing states traverse the South China Sea, making it a key strategic region, and potential trouble spot for the Chinese government. The PLA Navy regularly patrols the South China Sea and conflicting territorial claims in the region have periodically erupted into naval confrontations.

In a move that could further fuel tensions in the South China Sea, China will step up exploration for methane hydrate, which is drawing attention as a future source of energy. Research in summer 2013 led to the discov-

[33] Ibid, p. 9.
[34] Secretary of State Hillary Rodham Clinton, "On Energy Diplomacy in the 21st Century," Georgetown University, Washington D.C., U.S. Department of State, Office of the Spokesperson, Oct 18, 2012, http://iipdigital.usembassy.gov/st/english/texttrans/2012/10/20121018137692.html#axzz36IxWCtMm [accessed July 2, 2014]. See also: Charles Emmerson and Paul Stevens, "Maritime Choke Points and the Global Energy System," *Chatham House Briefing Paper*, January 2012, http://www.chathamhouse.org/publications/papers/view/181615 [accessed July 19, 2014].
[35] Captain Brian Wilson, U.S. Navy (ret.), "Maritime Energy Security." This Article was originally presented at NATO Centre of Excellence Defence Against Terrorism (COE-DAT) in Nov 2012 during the NATO SPS sponsored Critical Energy Infrastructure Protection (CEIP) Advanced Research Workshop (NATO ARW) and published by IOS Press in the ARW Book.
[36] Ibid, p. 5.
[37] Wikipedia, „String of Pearls (China)," http://en.wikipedia.org/wiki/String_of_Pearls_(China) [accessed July 4, 2014].

ery of a high-purity methane hydrate reserve in the northern part of the South China Sea, according to the Ministry of Land and Resources of the PRC. The reserve, sitting off the coast of Guangdong Province, is estimated to span 55 sq. km and amount to the equivalent of 100 to 150 billion cu. meters of natural gas.[38]

As China widens its search for methane hydrate in the South China Sea, it may create more friction with countries such as the Philippines and Vietnam. In a new official map, unveiled by Chinese state media on June 25, the PRC underlined its claims on the South China Sea showing continental China along with its self-declared sea boundary in the South China Sea stretching down to the coast of Malaysia, Vietnam and the Philippines.[39] China's neighbors will not be amused.

On May 5, 2014, Bloomberg reported that Vietnam denounced China for setting up an exploration rig in waters off its central coast disputed by the two countries. Vietnam said that the rig's placement is within its exclusive economic zone, citing its proximity to the Vietnamese coast. China's Foreign Ministry spokesman Hua Chunying told reporters that the oil rig was erected in Chinese territory.[40]

Previously these kinds of disputes tended to take place over survey ships but this time it is a drilling rig.[41] The dispute escalated very rapidly. At least 21 people were killed and nearly 100 injured in Vietnam on May 15 during violent protests against China. Crowds set fire to industrial parks and factories, hunted down Chinese workers and attacked police during the riots. The protests forced Chinese nationals to leave Vietnam because they didn't feel safe there.[42]

Surprisingly, the Chinese oil rig began moving on July 15. Rear Admiral Ngo Ngoc Thu, Vice Commander of the Vietnamese Coast Guard, said that the Chinese vessels that had been accompanying the rig were also moving. A spokesman of China Oilfield Services Ltd. (COSL) confirmed drilling work has been completed ahead of schedule and the rig's new intended location will be near China's island of Hainan, an area not disputed with other nations.[43]

In my opinion the new deployment of the rig is a tactical step by the Chinese government.

On one hand it could help to ease the tensions between China and Vietnam but on the other hand China will never give up its "right" to explore the contested waters.

[38] Gaku Shimada, "Chinese eye methane hydrate reserves in South China Sea," *Nikkei Asian Review*, April 24, 2014, http://asia.nikkei.com/print/article/27074 [accessed July 4, 2014].

[39] Ben Blanchard and Sui-Lee Wee, "China's Neighbors Are Not Going To Be Happy About This New Map," *Reuters*, June 25, 2014, http://www.businessinsider.com/r-new-chinese-map-gives-greater-play-to-south-china-sea-claims-2014-25 [accessed July 16, 2014].
See also: Lutz Feldt, "China's Strategic Maritime Ambitions – A European Perspective," International Relations and Security Network (ISN), Center for Security Studies (CSS), ETH Zurich, May 2013, http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=164160 [accessed July 23, 2014].

[40] Bloomberg, "Vietnam Protests Against China's 'Mobile Sovereign Territory' aka Deepwater Drilling Rig," *gCaptain*, May 5, 2014, http://gcaptain.com/vietnam-protests-chinas-mobile-sovereign-territory-aka-deepwater-drilling-rig/ [accessed July 4, 2014].

[41] Ibid.

[42] Kate Hodal and Jonathan Kaiman, "At least 21 dead in Vietnam anti-China protests over oil rig," *theguardian*, May 15, 2014, http://www.theguardian.com/world/2014/may/15/vietnam-anti-china-protests-oil-rig-dead-injured [accessed July 16, 2014].

[43] Brian Spegele and Vu Trong Khanh, "China Moves Oil Rig From Contested Waters," *The Wall Street Journal World*, July 16, 2014, http://online.wsj.com/articles/chinas-cosl-moves-oil-rig-from-contested-waters-1405472611 [accessed July 18, 2014].

On May 14, 2014 the Philippines' Department of Foreign Affairs said in a statement that it had lodged a formal protest with China on April 4 regarding the construction work at Johnson South Reef in the Spratlys. The protest was rejected by China saying that the "reef is Chinese territory."[44]

In an article titled *China Builds Artificial Islands in South China Sea*, Joel Guinto argues that artificial islands could help China anchor its claim to waters that host some of the world's busiest shipping lanes, referring to a 2013 report by the U.S. Energy Information Administration (EIA) that the South China Sea may hold as much as 11 billion barrels of oil and 190 trillion cubic feet of natural gas.[45]

Anyway, it is clear that disputes in the East and South China Seas cannot be solved by a single power or even by a group of small powers. Therefore cooperation between partners is a key to success, not only regarding the protection of the Sea Lines of Communication (SLOCs) but also to provide a stable maritime environment and stability in the production and delivery of energy.

The meeting of Admiral Jonathan Greenert, Chief of Operations U.S. Navy, in July 2014 with his counterpart Wu Shengli, Commander in Chief of the People's Liberation Army Navy (PLAN), focused on expanding cooperation and communication between their two navies. Wu called for cooperation in rescue missions and disaster relief, and implementing the Code for Unplanned Encounters at Sea (CUES), which was endorsed by the Western Pacific Naval Symposium in the Chinese city of Qingtao in April 2014.[46]

In my opinion the meeting will have little impact on strategic issues. The CUES isn't legally binding and Chinese ships will not necessarily observe it in their claims in the South China Sea or East China Sea. Building up person to person relationships, improving confidence building measures, establishing better and clearer communication mechanisms between the two navies and prevent any misunderstandings and miscalculations at sea, and offering China participation in this year's RIMPAC drills are steps in the right direction.

Already in 2002, member states of the International Maritime Organization (IMO) developed and implemented the International Ship and Port Facility Security (ISPS) Code. This agreement provides standardized procedures for evaluating risks. ISPS includes guidance on assessing ship and port facility security plans and monitoring and controlling people's access to such areas.[47]

The Container Security Initiative (CSI) program was developed to heighten container security. Under CSI, shipping containers that pose a terrorist risk are inspected in foreign ports before being transported to the United States. In part, CSI employs intelligence and automated information, pre-screening of cargo, and detection technology.[48]

[44] Trefor Moss, "China begins Construction in Spratly Islands," *World* News, updated May 14, 2014, http://online.wsj.com/news/articles/SB10001424052702304908304579561123291666730 [accessed July 16, 2014].
[45] Joel Guinto, "China Builds Artificial Islands in South China Sea," *Bloomberg Businessweek – Global Economics*, June 19, 2014, http://www.businessweek.com/articles/2014-06-19/china-builds-artificial-islands-in-south-china-sea [accessed July 16, 2014].
[46] Ankit Panda, "US Navy Chief Visits China," *The Diplomat*, July 16, 2014, http://thediplomat.com/2014/07/us-navy-chief-visits-china/ [accessed July 19, 2014].
Regarding the CUES see: http://news.usni.org/2014/06/17/document-conduct-unplanned-encounters-sea
[47] International Maritime Organisation (IMO), "ISPS Code," http/www.imo.org/ourwork/security/instruments/pages/ispscode.aspx [accessed July 4, 2014].
[48] Department of Homeland Security, "Container Security Initiative Ports," http://www.dhs.gov/container-security-initiative-ports [accessed July 4, 2014].

Along with multinational efforts and international partnering, the private sector plays a pivotal role in *maritime energy security*. In the United States, the private sector owns more than 80% of the energy infrastructure which includes 150 refineries, 4,000 offshore platforms, 160,000 miles of oil pipelines, 10,400 power plants, 410 underground storage fields, and 1.4 million miles of natural gas pipelines.[49]

Threats to maritime energy security aren't solely from illicit activities; natural disasters and aging infrastructures also adversely effect energy security. Remember hurricanes Katrina and Rita shut down 94% of the oil production in the Gulf of Mexico's outer continental shelf, which comprises 7% of U.S. consumption. Or remember typhoon *Haiyan* in the Philippines in November 2013 creating destruction and sending a strong message that the world is unprepared for the violence of climate change.

The European Intelligence Analysis Centre

Finally, some remarks about the European Intelligence Analysis Centre, the EU INTCEN, the intelligence body of the European Union, are appropriate. Since January 2011, the EU INTCEN is part of the European External Action Service (EEAS), under the authority of the High Representative of the Union for Foreign Affairs & Security Policy, Baroness Catherine Ashton.[50] Her mandate will end on October 31, 2014 and the position will be replaced by the end of 2014.

The mission of the EU INTCEN is to provide intelligence analyses, early warning and situational awareness to the High Representative Catherine Ashton and to the European Action Service, to the various EU decision making bodies in the fields of Common Security and Foreign Policy and the Common Security and Defence Policy and Counter-Terrorism, as well as to EU Member States.

EU INTCEN does this by monitoring and assessing international events, focusing particularly on sensitive geographical areas, terrorism and the proliferation of weapons of mass destruction (WMD) and other global threats.

As of 2012, the EU INTCEN is composed of two divisions:

- The Analysis Division is responsible for providing strategic analyses based on input from foreign and security intelligence services of the Member States. It is composed of various sections, dealing with geographical and thematic topics.
- The General and External Relations Division looks at all legal and administrative questions, and produces open-source analyses. It is composed of three sections dealing respectively with IT questions, internal and external communication, as well as the open source office responsible for Open Source Analysis.

Inquiries by EU INTCEN concerning topics such as crises, developments in given states and regions and terrorist threats, etc. are sent via the national experts to the foreign intelligence and/or security services, using the form of an official request for information (RFI). The services then have the discretionary power to decide whether and

[49] Brian Wilson, "Maritime Energy Security," *SSRN Social Science Research Network*, Nov 1, 2012, p. 9, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229989 [accessed July 4, 2014].
[50] Wikipedia, „EU Intelligence Analysis Centre (EU INTCEN)," http://en.wikipedia.org/wiki/EU_Intelligence_Analysis_Centre_(EU_INTCEN) [accessed July 23, 2014].
See also: Björn Müller-Wille, „For our eyes only? Shaping an intelligence community with the EU," Institute for Security Studies, Occasional Papers, no. 50, Paris, January 2004.

to what extent they wish to or can respond to the EU INTCEN's inquiry. It goes without saying that each service respects the privacy of its sources.

Merging both civilian and military information, these contributions are then used to produce all-source intelligence assessments. This *modus operandi* has the following advantages:

- Intelligence information from different intelligence and security services, with different capacities, is merged;
- The overall knowledge basis is extended;
- The perceived threat is uniformly monitored;
- The common analysis process is fostered and joint political decisions are supported.

The EU INTCEN maintains also ties with the EU Satellite Centre in Torrejón, Spain,[51] with EUROPOL in The Hague,[52] with the European Union Institute for Security Studies (EUISS) in Paris,[53] with the Foreign Offices of the Member States, the EU Special Representatives[54] in given regions, as well as experts in the Policy Unit and in the Council Secretariat.

The present Director of the EU INTCEN is Ilkka Salmi, previously Head of the Finnish Security Intelligence Service. The center has around 70 employees.

Conclusions

Let me conclude:

- If we understand security policy in a more comprehensive way, that means the political, economic, social, ecological and military dimensions must be considered together and must be brought together, then maritime terrorism, piracy and armed robbery and potential threats in the field of maritime energy security can only be fought successfully in cooperation between state institutions and the private sector.
- Good intelligence in the maritime domain will be a prerequisite for combating potential threats including the collection of political, economic and military information.
- Multinational patrols, increased safety measures adopted by shipping companies and private security guards on board of ships led to a significant drop of piracy and armed robbery off the Somali coast and off the Horn of Africa in 2013.

[51] EEAS European Union External Action Service, "European Union Satellite Centre (Torrejón)," http://eeas.europa.eu/csdp/structures-instruments-agencies/eu-agencies-on-csdp/eu-satellite-centre/index_en.htm [accessed July 23, 2014].
[52] EUROPOL, https://www.europol.europa.eu/ [accessed July 23, 2014].
[53] EUISS European Union Institute for Security Studies, http://www.iss.europa.eu/ [accessed July 23, 2014].
[54] EEAS European Union External Action Service, "EU Special Representatives," http://eeas.europa.eu/policies/eu-special-representatives/index_en.htm [accessed July 23, 2014].

- West African piracy will remain the most active in terms of the number of attacks in 2014 and in the foreseeable future.
- In Southeast Asia it has to be seen whether oil related attacks on ships will increase, inspired by successful piracy attacks off the West African coast.
- In 2014, low level attacks in Southeast Asia will likely continue because attacks against ships in harbours or slow moving vessels in very narrow waters are easy targets for pirates and other criminals.
- Also in the future energy will be essential for the security of nations for economic stability and global trade. The critical energy infrastructure has been and will be in the sights of terrorists.
- The Sea Lines of Communication (SLOCs), connecting China and other Northeast Asian states to the Middle Eastern oil producing states traverse the South China Sea and are of great strategic importance. Further disputes between China and other claimants regarding islands in the East and South China Sea can be expected because all of them want to profit from the rich energy resources in this strategic region.

Recommendations

Finally, some recommendations:

1. States should analyze how the different Intelligence and Security Services and other institutions could improve cooperation.
2. Develop a watch list and establish priorities to analyze present and future threats relevant for the country and the region.
3. Open-Source Intelligence (OSINT) could strengthen the knowledge base.
4. Bundling Information could be a key to success.
5. Analyze Internet websites, e-mail traffic and other means of communication of potential terrorists.
6. Improve information sharing between selected countries in Asia, the European Union, the United States, Latin America and Africa, mainly with Foreign Intelligence and Security Services.
7. Use the regional expertise on information regarding the maritime domain and other issues to “trade information” with Foreign Services.
8. Evaluate the proposal of the United States for closer intelligence cooperation between Washington, Tokyo and Seoul.
9. Dedicate more resources to counter intelligence.
10. Improve encryption systems.
11. More involvement of the private sector is necessary.

12. Raise the awareness of decision makers in politics, in the armed forces, in the business sector and in public for potential threats in the field of economic and industrial espionage, including threats in the maritime domain.

***

Remarks: Opinions expressed in this contribution, finalized on July 25, 2014, are those of the author.

The present paper was written for the office of the Konrad Adenauer Foundation Rio de Janeiro (KAS), and comprises part of this year's edition of the forthcoming publication *Forte de Copacabana*, in October 2014. The publication, the thematic focus of which centres on international security, accompanies the international security conference of the same name, viz., "*Forte de Copacabana*", which is the 11th such event. The above conference is scheduled to take place in Rio de Janeiro, Brazil, on October 10, 2014. For further information, please visit the KAS Brazil website at: https://www.kas.de/brasilien/

About the Author

Dr. Peter Roell has been president of the Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) in Berlin since January 2006. His previous appointments were as senior advisor for foreign and security policy at the Permanent Representation of the Federal Republic of Germany to the EU in Brussels. In Germany, Dr. Roell served as director of the Asia-Pacific, Latin America and Africa (Sub-Sahara) branch and at German embassies in the Near and Middle East and in Asia.

Dr. Roell studied sinology and political sciences at the universities of Bonn, Taipei and Heidelberg. He gained his Ph.D. from the Ruprecht-Karls-University in Heidelberg.

Dr. Roell is an ancien of the NATO Defense College in Rome and the Federal College for Security Policy Studies (BAKS) in Berlin.

Dr. Peter Roell