

VOLUME 7 ISSUE 2

DEFENSE SECURITY BRIEF

December 2018



Institute for National Defense and
Security Research



Institute for National Defense and
Security Research

Military Cyber Threats and Responses 1

Ma Ying-han

The Critical Role of Crisis Resilience
in Building and Sustaining Political,
Economic and Social Stability 17

*Benjamin J. Ryan, Deon V. Canyon, James
Campbell, Frederick M. Burkle, & Wie-Sen Li*

Reflections on the Rise of China's Navy 39

James Goldrick

The United States Seventh Fleet Patrol
and Taiwan : Past and Present 51

Catherine Kai-ping Lin

ISSN 2225360-2

INDSR

The Institute for National Defense and Security Research (INDSR) is dedicated to fueling knowledge-based policy analyses and strategic assessments on Taiwan's security. Our mission is to safeguard Taiwan's democracy and prosperity by strengthening mutual understanding and advancing common interests in the defense and security community both globally and at home. INDSR was formally inaugurated on May 1, 2018, and is headquartered in Taipei, Taiwan. We are an independent, nonpartisan, nonprofit organization.

LEADERSHIP

Kent Feng (Chairman) Cheng-Yi Lin (President) Chyungly Lee (Vice President)

DEFENSE SECURITY BRIEF

Defense Security Brief (DSB) is an English-language publication aimed at strengthening research exchanges with security-related experts both domestically and abroad. Established in 2011, DSB was originally founded and compiled by the Office of Defense Studies, Ministry of National Defense. INDSR continued the publication in 2018.

EDITORS

Si-Fu Ou (Editor in Chief)

Catherine K.P. Lin	Chih-Sion Sheu	J.R. Wu	Oddis Jung-Feng Tsai
Po-Chou Lin	Ruo-Min Chou		

OFFICE

Institute for National Defense and Security Research

No.172, Bo-Ai Road, Chongcheng Dist., Taipei City, Taiwan (R.O.C.)

Tel: 886-2-2331-2360 Fax: 886-2-2331-2361

Printed in Taiwan

ISSN 2225360-2

Copyright © 2018 The Institute for National Defense and Security Research

Cover photo: R.O.C. Army's armored vehicle. (Source: Hsiao-Huang Shu/INDSR)

Military Cyber Threats and Responses

By Ma Ying-han

Commander Ma delivered this speech as the lunch keynote on October 8, 2018, at the 2018 Defense Forum on Regional Security, which focused on the theme of “New Security Challenges in the Indo-Pacific Region: Cybersecurity Governance and China’s Sharp Power”. The speech was delivered in Mandarin. It is translated here into English by J.R. Wu.

Mr Chairman, distinguished guests, good afternoon.

My name is Lieutenant General Ma Ying-han. I am the Commander of the Information Communications and Electronic Force Command of the Ministry of National Defense. It is my great pleasure to be invited to speak at the “2018 Defense Forum on Regional Security”. I’m going to talk about the issue of “Military Cyber Threats and Responses”. But before I begin my report, let me give a brief introduction of myself.

This is a short curriculum vitae of myself. I will let you read for yourself my education. As for my career, I have worked in the General Staff Headquarters in recent years. I have been a Director of information security for J6, Commander of the Joint Information Operation Command, and Director of the Army’s communication information division G6.

My presentation today includes five sections, which I am going to report on to the scholars and guests here. Including the preface and conclusion,

I am going to talk about international cyber threats and trends, the development and intentions of the PLA's cyber corps, and Taiwan's cyber security defense strategy.



Information Communication Electronic Force, the fourth branch of the R.O.C. armed forces, has been established on June 29, 2017. (Source: R.O.C. Military News Agency)

With the advancement and development of technology, the tools of human communication are constantly evolving and the importance of the Internet is beyond words; there are those who would use it to deliberately deceive, steal and destroy in order to influence a country's politics, economy, psychology and military, or to achieve a criminal purpose. Its influence crosses modern sovereignty and governance, making cyberspace a new type of space that is different from land, sea, air and outer space.

Nowadays, the image of the mobile device represents access to all-inclusive services. With the touch of a finger, personal needs are met (knowledge), but at the same time there is high cyber security risk.

Let's turn to the first section: international cyber threats and trends. With one word leaked out, the cover of an entire military is wiped out. It may be just a one-click mistake, but it will never be recovered.

The United States' *2018 Department of Defense Cyber Strategy* report clearly stated that the openness, trans-national, fragmented nature of the Internet creates serious vulnerabilities. Based on *The Global Risks Report 2018* by the World Economic Forum, cyber attacks have risen to be the number three risk this year, jumping from number six in 2017.

Among the top five risks listed, three of them are related to the environment. The other two are cyber attacks and data fraud or theft. According to an October 5 article by Bloomberg's Business Week, a micro-chip as tiny as a sharpened pencil tip was implanted during a specific stage of the supply chain production of Super Micro Computer Inc., that collected and stole data, reportedly affecting more than 30 enterprises. This goes to show that, in the future, the risks of the virtual world are becoming more and more difficult to identify.

Let's take a look at the trends in cyber threats.

According a report by the European Union Agency for Network and Information Security (ENISA) issued at the beginning of this year, malware, web-based attacks, web-application attacks, phishing and spam were ranked at the forefront of cyber threats. In particular in late 2017, the discovery of ten vulnerabilities in the WPA2 (Wi-Fi Protected Access) security protocol and the KRACK (Key Reinstallation Attack) attacks allowed hackers to systematically crack Wi-Fi network

passwords, then eavesdrop on the content, kidnap the connection or launch an attack.

Although at this year's International Consumer Electronics Show (CES), the Wi-Fi Alliance announced the new WPA3 security protocol, current Wi-Fi hotspots cannot all be transformed overnight. Special care should be used when accessing public, password-less Wi-Fi hotspots.

Now let's take a closer look at hackers using the above attack techniques and what they are after.

According to an article on May 28 in Taiwan's Liberty Times, in order to obtain and grasp the information on the military insurance and health insurance of Taiwan's military personnel, their relatives and of the general public, the Chinese Communist Party (CCP) has repeatedly wanted to break into the website of our military hospitals and steal military medical records. Based on statistics, last year there were more than 162.45 million of such attacks.

In addition, the well-known global social media Facebook recently disclosed that last month on the afternoon of September 25 it discovered a security problem. Attackers exploiting vulnerabilities in the system could access user accounts, directly affecting 50 million accounts. Ninety million users had to re-login.

It is clear that in recent years, no matter if it is an official government or non-government institution, the theft of personal data is still one of the main objectives of hacking organizations. Because personal data can be used in many ways, nothing is beyond what they can accomplish, even if you cannot imagine it.

So apart from personal data, what else do they want? Let's look further.

Here domestically, from the ATM heist of First Commercial Bank to the hacking of Far Eastern International Bank, those cases show hackers intruding into the dedicated financial telecommunications networks used by financial institutions. Just like a movie plot, NT\$1.8 billion in funds was transferred out, a success, and no handling fee charges.

CCP's cyber corps is not only composed of military units, but also a large number of peripheral civil organizations.

When the Wannacry ransomware happened, U.S. media cited South Korean scholar Boo Hyeong-wook as describing, this is what North

Korean hackers do. They loyally extort large sums of money for their government. The FBI recently filed charges on this case. They are convinced the Wannacry ransomware was carried out by the North Korean hacking group Lazarus. Therefore, the purpose of an incursion is not solely for stealing personal data. Money is another great incentive.

We have the threat trends, the methods, the purpose. Where is the source?

On April 5, 2018, the Executive Yuan's Department of Cyber Security stated that public offices are hit by cyber attacks over 20 million times a month on average, and at most over 40 million times a month. Although the volume of attacks is gradually trending down, the success rate of these attacks is on the rise. According to Cisco's Talos, its threat intelligence organization, a single hacking group (the Russians who initiated the VPNFilter malware) has infected more than 500,000 routers worldwide, showing that the methods of cyber attacks are constantly evolving into something new. Meanwhile, high-risk

networking equipment has become the optimal method of hackers on the other side of the Taiwan Strait.

The Executive Yuan pinpointed that among the cyber attacks that Taiwan suffers, 80% of them are from the CCP. Its “attack and scare” tactics not only occur in tangible space, but more and more also in the cyber space where it pokes holes through the walls, virtually, to press its advantage. Looking at the CCP’s cyber corps development and intentions, we can make a further analysis:

How many times on average is Taiwan’s Ministry of National Defense attacked each year? In 2017, 734,502 times. That’s 61,208 times on average a month. For 2018 so far, it has been 678,318 times, or averaging 75,368 times a month. In this case, it is trending higher.

Under the goals of the CCP’s 2015 “China Dream” and “Strong Military Dream”, with the “Small Leading Group for Deepening the National Defense and Army Reform” at its core, the planning for the structural reform of the military and related details abolished the four major headquarters in 2016. It also reorganized the high-level divisions and consolidated the seven major military regions into five major theaters.

An original 11-level command system was simplified to a three-level command system. Think of the changes like this: What had been “individual” horse-drawn carriages were transformed into a single chariot being powered by many horses to increase its “unified strength.”

So what kind of organization holds the reins of so many horses? Let’s look at the next page – the Three-Level Command System: Joint Strategy Command, Operations Command, and Brigade.

The most noteworthy, of course, is that the CCP established a Strategic Support Force on December 31, 2015, that included the former General Staff Department's Third Department (and GSD's Fourth Department and Fifth Department), as well as other units involved with electromagnetics, cyber and aerospace. Its main mission is to provide joint operations with "accurate, efficient and reliable information to guarantee strategic support." In other words, the CCP's Strategic Support Force is like the reins pulling many horses in the picture, effectively integrating the strategic support forces with the theaters and forming the core of joint warfare.

This kind of plan resonates with what was in the US Department of Defense's 2018 cyber strategy report. The US report disclosed that "the joint forces will adopt cyber attack capabilities and innovative concepts, and conduct cyberspace operations in full spectrum conflicts." This is possibly the new benchmark for various countries as they develop warfare capabilities in cyberspace in the future.

What does the face of the cyber corps supporting the force look like?

Everyone knows that the CCP's cyber corps is not only composed of military units, but also a large number of peripheral civil organizations. These are mostly units cultivated by the People's Liberation Army (PLA). Reviews by CrowdStrike, Mandiant and FireEye, three cyber firms in the US, inferred that hacker groups in China, based on the behavior patterns of their cyber attacks, the techniques and tools they used, tied them to the CCP's cyber warfare forces.

Among the dozens of hacker organizations, CrowdStrike identifies those with close interaction with the PLA under the variant of the "****panda" name, for example "Deep Panda"; Mandiant uses an "APT X" identifier,

for example APT-19 (Winnti umbrella); FireEye doesn't utilize specific naming rules. What is currently certain is the relationship between Unit 61398 and Unit 61486 of the PLA, and these civil or private hacker organizations is extremely tight.

Let's look at what they have done and their intentions.

This chart is an excerpt. It is summary statistics of intrusions by China's cyber corps into Taiwan's public sector prior to 2013 (these are publicly available information). We can see that between 2008-2011, in these three years, there were 4 cases. Between 2011-2013, these two years, there were 7 cases. In 2013, alone, there had been at least 8 cases. There has been a large amount of data that has been leaked, leading to various policy developments being detected by the enemy in advance and then in turn employed by various strategies targeting Taiwan. This is the first intention of the PLA's cyber corps.

Cybersecurity intelligence firm FireEye on Jun 21 this year released *M-Trends 2018* in Taiwan. The report showed that the dwell time (the number of days from first evidence of compromise that an attacker is present on a victim network before detection) for Asia-Pacific enterprises was four times the global median (498 days to 101 days).

Many industries in Taiwan have repeatedly suffered from attacks suspected of being cyber espionage activity from China. Chinese hackers like to use Taiwan as a testing ground for sophisticated cyber-spyware technology. Many experimental malware will be first launched in attacks against Taiwan before they are used to attack American companies. This is the second intention of the PLA cyber corps.



Taiwan have repeatedly suffered from attacks suspected of being cyber espionage activity from China. (Source: R.O.C. Military News Agency)

In addition to data theft, destruction and other kinds of cyber attacks, the most distinctive mode of operation in recent years is the CCP's "50 Cent Party" (中共五毛黨; colloquial term for Internet commentators hired by Chinese authorities to manipulate public opinion to the benefit of the CCP). These commentators are employed to publish articles on the Internet in favor of the Chinese government, while at the same time besiege their online critics. Recently the most common trick has been to publish fake news to achieve the purpose of mis-leading online public opinion. However, in the near future, this work may be partially replaced by artificially intelligent editing robots.

In September after US President Donald Trump at the UN Security Council accused China of meddling in the US 2018 mid-term elections, he tweeted China was placing ads in Iowa media and other newspapers

to spread propaganda that the US trade war against China was hurting the interests of American farmers, with the intent to interfere in the US midterm elections.

Bloomberg also reported in September, Taiwan's Executive Yuan's cyber security department chief Howard Jyan stating that hacker groups

Chinese hackers like to use Taiwan as a testing ground for sophisticated cyber-spyware technology.

will try to interfere during our November's local elections. We believe this is the PLA's cyber corps third intent.

In summary, the intentions are to understand the enemy's extreme weaknesses for source of threats in cyberspace, in order to build up the combat capabilities, while also understand the nature of its own

vulnerabilities, in order to develop appropriate security policies.

Now let us turn to how Taiwan has been enhancing its cyber security defense strategy.

The latest summary on cyber strategy by the US government identifies China and Russia as the top threats in cyber security. There is no doubt about this.

Addressing this close-at-hand threat, Taiwan's National Security Council and the Executive Yuan on August 27-28, 2016, held a strategic conference on "Cyber Security Is National Security." This opened the opportunity for settling major national strategy and continued the 3X3X3 national-level cyber security strategy.

President Tsai, on June 29, 2017, presided over the ceremony of our command (Information Communications and Electronics Force Command). She said: “As the Ministry of National Defense enters the era of comprehensive information warfare, the threat comes not only from territories with borders, but more threats come from cyberspace. The harm to national security from cyber threats is not any less than traditional armed attacks.” Therefore, the government not only established the Executive Yuan’s Department of Cyber Security, but also established the Information Communications and Electronics Force Command as specific actions of “Cyber Security Is National Security.”¹

I personally see that under the framework of our *National Cyber Security Strategy Report* that to continue to improve the cyber defense of our military, we must implement intelligence integration (know the enemy), have multi-layered defense (defend against the enemy), set a methodology for educational training (win against the enemy), in order to form a formidable force, effectively defending the country's digital territory.

Let’s continue further to look at the framework of intelligence-driven national cyber joint defense.

According to our national *Cyber Security Strategy Report*, the joint defense system of our national cyber security comprises of three levels: the government, critical information infrastructure areas and providers. This joint defense system includes national security units and cabinet agencies and ministries forming and integrating teams for emergency response, early warning, notification and processing to set up a cyber

¹ *National Cyber Security Strategy Report*, ICT Security of National Security Council, September 14, 2017, <https://www.president.gov.tw/File/Doc/8f65b086-6be5-4481-b376-a4001204f003>

security joint defense framework for “information sharing, collaboration and response”. This enhances the capabilities and effectiveness of early warning, emergency response and continuous operations.



A new National Cyber Security Strategy Report provided by ICT Security of National Security Council, September 14, 2017. (Source: R.O.C. Military News Agency)

The cyber defense of Taiwan’s military also needs the technology, experience, connections and exchanges with the outside world. Within the national cyber security joint defense mechanism, our cyber command force – apart from carrying out the good work in protecting the cyberspace within our own military – we are also part of the Executive Yuan’s push to integrate and establish the cyber security joint defense and intelligence sharing system of critical information infrastructures.

We are actively absorbing Europe, the US and other advanced countries’ coordination in Defense Critical Infrastructure (DCI) and Defense

Industrial Base (DIB) operational mechanisms, to achieve a broader early warning system and more rapid response capabilities.

Apart from the mission of coordination of information and of critical infrastructure, what are the cyber security defense concepts of our cyber command?

Currently, the US military is orienting itself from a “zero-defect culture toward one that is increasing its innovation and agile response capabilities.” In addition to the integration of sophisticated equipment and technology, we also focus on multi-layered defense, forensic knowledge and rapid recovery, because only from an invincible position, we can talk about the development of military cyber combat power. Distinguished guests, if you pick up a piece of cheese, you will see that there are many holes in the surface of the cheese because of the fermentation. But as long as the cheese is thick enough, you will not be able to see through it.

From the perspective of cyber security, no security protection system is perfect, but as long as multiple defenses are formed, various security risks cannot form a straight line, and cyber defenses will not be broken. We must build a multi-layer cyber security defense, from the information server to the network node to the terminal equipment. That is, from the cloud to the terminus, the all-round information security environment, so that the enemy cannot enter, cannot take, and cannot unlock to achieve his goal to make a tiny change or chain reaction.

So how do we form a formidable combat force?

Combat power is the basis for victory. From the perspective of overall combat power, we must consolidate cyber security defenses and continue to strengthen cross-domain cooperation alliances to build

solid multi-layered deterrence capabilities. The strategy of our systematic education and training is to require the troops to pass the test of three levels of professional licenses, establish basic knowledge, and then train in six professional areas of cyberspace (program development, operating systems, network equipment, databases, web systems and cryptography). These stages focus on the combination of theory and practice, and the final stage is a Level Three specialization training course, utilizing the expert-level capabilities of the military.

Usually, we participate in the national-level cyber attack drills and special projects of various ministries of the Executive Yuan. We review the effectiveness of the capabilities, combat equipment and training, and then adjust the training program to grow combat power and – with the government’s cyber security team – together give play to our national-level joint cyber defense warfare.

Finally, let me offer a brief conclusion.

The latest September issue of one of our defense publications examined an article from a defense bi-monthly in the US that discussed *Sun Tzu's Art of War* in the use of cyber warfare. The article takes the thirteen chapters of *Sun Tzu's Art of War* to interpret cyber warfare, strategy and tactics. From this, came some interesting and appropriate links.

For example, the chapter on Tactical Dispositions: The skillful fighter puts himself into a position which makes defeat impossible, and does not miss the moment for defeating the enemy.

The author believes the information system must have the resilience to withstand attacks and be invincible. When taking action in cyber security defense, we must follow the decision cycle of “observe, orient, decide, act ” (OODA) to respond and defeat the cyber attack. In the

future, cloud technology will become the basic framework for the Internet of Things, combat management and information transfer. From the cloud to the terminus, cyber security is a holistic issue.

Let me use the rigorous and shifting Bagua structure in Chinese culture to convey an all-round cyber security concept. The core of Bagua is the Taiji philosophy, the yin and yang principles. The core of harmonious operations in cyberspace is – information security, and its yin and yang are "convenience and risk" complementing, interacting, shrinking and growing with each other.

Yin and yang then grows in four directions, and extending the metaphor for maintaining cyber security is the ISO-27001 international information security standard with the four major steps in risk prevention of "Plan, Do, Check, Act" (PDCA) to allow for a continuous cycle of corrective measures.

Finally, the eight trigrams, the metaphor is the Certified Information Systems Security Professional (CISSP) – security and risk management, asset security, security architecture and engineering, communication and network security, identity and access management, security assessment and testing, security operations, and software development security, make up the eight faces.

These form "all-round information security" so that it can achieve in cyberspace what *Sun Tzu's Art of War's* Tactical Dispositions (Chapter 4) says: The skillful fighter puts himself into a position which makes defeat impossible, and does not miss the moment for defeating the enemy.

Lieutenant General Ma Ying-han is the Commander of the Information Communications and Electronic Force Command of the Ministry of National Defense, R.O.C. He was the Director of Communications, Electronics and Information Division of the Army Command of the Ministry of National Defense, R.O.C. He has a Master' s degree in information management from Yuan Ze University College of Informatics.

The Critical Role of Crisis Resilience in Building and Sustaining Political, Economic and Social Stability

By Benjamin J. Ryan, Deon V. Canyon, James Campbell, Frederick M. Burkle, and Wie-Sen Li

Introduction

The increasing complexity, and multidisciplinary and transboundary nature of modern-day crises require the security sector to work with those in clinical care, public health, diplomacy, law, politics and the social sciences to build and sustain stability across the Indo-Pacific. The 2030 Sustainable Development Agenda, including the Sendai Framework for Disaster Risk Reduction (SFDRR), the Sustainable Development Goals, the Addis Ababa Action Agenda, the Paris Agreement on climate change and the New Urban Agenda provide a platform for the security sector to actively support political, economic and social stability.¹ The 2015 SFDRR for the first time established community “resilience” and well-being as an explicit outcome.² The 2005 Hyogo Framework for Action (HFA) signed by 168 nations, also

¹ UNISDR, *Disaster Resilience Scorecard for Cities* (Geneva: United Nations Office for Disaster Risk Reduction, 2017); UNISDR, *How to Make Cities More Resilient - A Handbook for Local Government Leaders* (Geneva: United Nations, 2017).

² Frederick M. Burkle, Shinichi Egawa, Anthony G. MacIntyre, Yasuhiro Otomo, Charles W. Beadling & John T. Walsh, “The 2015 Hyogo Framework for Action: Cautious Optimism,” *Disaster Medicine and Public Health Preparedness*, Vol. 8, Issue.3(2014), pp.191-192.

called on “specific actions” focused on “building the resilience of nations and communities through disaster risk reduction, improving risk information and early warning, building a culture of safety and resilience, reducing risks in major sectors and strengthening preparedness for response”.³ These agreements recognize the important role all sectors and levels of government can play in development, which underpins resilience.⁴ Successful implementation depends on a whole-of-society partnership.

For the Indo-Pacific to build and maintain crisis resilience, implementation is required at regional, national, provincial and local levels. However, without a resilient local government and community, national and provincial resilience is not possible. This is because the local community levels are most intensely and immediately impacted by a crisis. The first responders work and live in communities affected and are best placed to understand the context that shapes their priorities and needs. All communities are different, with varied geography, critical infrastructure and population risks and vulnerabilities. Enhancing community resilience and taking responsibility for that resilience extends to the “anticipation and assessment of threats”.⁵ Ultimately, resilience depends on the capacity, competence and willingness of local

³ Frederick M. Burkle, “Hyogo Declaration and the cultural map of the world,” *Disaster Medicine and Public Health Preparedness*, Vol. 8, No.4(2014), 280-282.

⁴ UNISDR, *Disaster Resilience Scorecard for Cities*, UNISDR, *How to Make Cities More Resilient - A Handbook for Local Government Leaders*.

⁵ Peter Rodgers, “Development of resilient Australia: enhancing the PPRR approach with anticipation, assessment and registration of risks,” *The Australian Journal of Emergency Management*, Vol. 26 (2011), pp. 56-58.

governments and their communities to sustain and advance strategies that integrate crisis mitigation and adaptation.⁶

Figure 1 - Crisis resilience model



Source: Ryan & Campbell, *Comprehensive Crisis Management for Security Practitioners: Structures, Systems and Policies* (Honolulu, HI: Daniel K. Inouye Asia-Pacific Center for Security Studies, 2018).

Key characteristics of a resilient local government include the ability to resist, absorb, accommodate, adapt to, transform and recover from the shocks of a hazard in a timely and efficient manner (Figure 1).⁷ In this context, a hazard is a process or phenomenon (for example, cyclone, earthquake or ecosystem decline) that may cause loss of life, injury or other health impacts, property damage, social and economic disruption or environmental degradation.⁸ Increasingly in the context of cities,

⁶ UNISDR, Implementation guide for local disaster risk reduction and resilience strategies - Public consultation version (Geneva: United Nations Office for Disaster Risk Reduction, 2018).

⁷ "Terminology," UNISDR, Retrieved December 27, 2017, from <http://www.unisdr.org/we/inform/terminology#letter-r>

⁸ Ibid.

resilience is framed around the ability to withstand and bounce back from chemical spills, power outages, as well as chronic stresses occurring over longer time scales, such as land salination, groundwater depletion, deforestation, or socio-economic issues such as homelessness and unemployment.⁹

Urbanization and the complex characteristics of local governments can present opportunities for crisis resilience, while at the same time they have the potential to increase vulnerabilities and risk.¹⁰ For example, 80% of the world's largest cities are vulnerable to severe impacts from earthquakes, 60% are at risk from storm surges and tsunamis, and over 50% of the world's population now reside in cities, with this expected to increase to 66% by 2050.¹¹ Rapid urbanization, common to the Indo-Pacific puts pressure on land and services if not accompanied by sustainable planning and appropriate land-use decisions. Rapid unsustainable urbanization occurs where incoming populations settle in hazard-prone areas such as coastal lowlands, floodplains or unstable and steep slopes.¹² The individuals and households in these populations experience reduced resilience compounded by compromised local infrastructure, which increases the risk of a destabilization and even societal collapse.

⁹ UNISDR, *Disaster Resilience Scorecard for Cities*, UNISDR, *How to Make Cities More Resilient - A Handbook for Local Government Leaders*.

¹⁰ Ibid.

¹¹ "Resilience," UN-Habitat, Retrieved December 27, 2017, from <https://unhabitat.org/urban-themes/resilience/>

¹² UNISDR, *Disaster Resilience Scorecard for Cities*, UNISDR, *How to Make Cities More Resilient - A Handbook for Local Government Leaders*.

Large urban areas also represent complex systems of systems, dependent on robust, uninterrupted, external connectivity for transportation, commerce, energy, communications, food, water and other resources. This interdependency creates unique public health vulnerabilities, such that a shock that is large enough and central enough to the national government and key societal institutions can spread like contagion through interconnected systems, potentially even leading to catastrophic failure of fragile states.

To provide a basis on which to build and sustain political, economic and social stability across the Indo-Pacific through resilience, this paper describes: crisis resilience; the importance of engaging local governments; benefits for the security sector; strategies to build and sustain resilience; and recommendations to enhance political, economic and social stability.

What is Crisis Resilience?

There are four interacting theoretical dimensions, which make relatively equal contributions to achieve the concept of crisis resilience (Figure 2). These include the level of: community linkage (e.g. social connectedness and cohesion); threats and vulnerabilities (e.g. risk of exposure to disaster, drought, famine, health status and unemployment); crises management (e.g. command, control and coordination structures); and present and absent resources (e.g. forests, food supply, education, employment and water). All local governments possess these dimensions to varying degrees and are used to respond to one or more disruptive events. However, if weakened to the point of failure, crisis resilience deteriorates as indicated in Figure 2, increasing the risk of destabilization and societal collapse. Weakening factors such as climate extremes, rapid unsustainable urbanization, critical

biodiversity loss, and scarcities of food, water and energy have accelerated these risks, further compounding vulnerabilities introduced by conflict and internally displaced and refugee populations, who already suffer from an absence of basic resiliency necessities such as shelter, food and a minimal income security.¹³

Figure 2 - Resilience dimensions



Source: Ryan & Campbell, *Comprehensive Crisis Management for Security Practitioners: Structures, Systems and Policies*

The United Nations International Strategy for Disaster Risk Reduction (UNISDR) describes key aspects of resilience in its publication *How to Make Cities more Resilient – A Handbook for Local Government Leaders*.

¹³ Frederick M. Burkle, "Current Crises & Potential Conflicts in Asia and the Pacific Health by a Different Name," Presented at the "Institutional Coordination in Disaster Management in the Asia Pacific" Conference 9 -10 April 2018, University of California at Berkeley APEC Study Center & the University of California San Diego Medical School.

In addition to promoting strong leadership, clear coordination structure and delineated responsibilities, the features of resilience include:

Feature	Dimension
Well-defined policies and strategies, including stakeholder engagement and effective communication	Crises management; community linkage
Routinely conducted risk assessments are required to improve knowledge about hazards to inform decisions on planning, development and investment	Threats and vulnerabilities
Financial plan that complements and promotes resilience activities	Crises management
Planning uses up-to-date risk information with a focus on the most vulnerable groups	Community linkage
Building regulations are realistic, compliant and enforced	Crises management; community linkage; present and absent resources threats
Ecosystems are identified, protected and monitored to sustain their function as a natural buffer	Crises management; community linkage; threats and vulnerabilities
Institutions relevant to resilience (for example, health services, transport infrastructure, electrical grid, water quality, sanitation systems and universities) have the capabilities to fulfil their functions	Crises management; community linkage; present and absent resources threats and vulnerabilities
Social connectedness and a culture of help nurtured and strengthened through	Crises management; community linkage;

education, events and communication through multi-media channels	
Strategies in-place to protect, maintain and upgrade critical infrastructure to ensure services can continue before, during and after a crisis	Crises management; present and absent resources
Preparedness plans, including early warning systems and public preparedness exercises, in-place to ensure an effective response and recovery	Crises management
Recovery strategies aligned with long-term planning	Crises management; community linkage; present and absent resources

Benefits for the Security Sector?

The security sector includes the structures, institutions and personnel responsible for the management, provision and oversight of security such as defense, law enforcement, corrections, intelligence services and institutions responsible for border management, customs and civil emergencies.¹⁴ This sector must consider the broader benefits wherein crisis resilience builds and sustains political, economic and social stability. This includes understanding the relationship between ecosystem and built environment stressors and security sector risks (Figure 3). For example, deforestation or wildfire increases susceptibility to flash flooding and landslides and reduce the carrying capacity for game. Thus, deprived (and often inadequately insured)

¹⁴ United Nations, "Security Sector Reform," Retrieved September 24, 2018, from <https://peacekeeping.un.org/en/security-sector-reform>

communities lose gardens and hunting grounds, and may not be able to rebuild their homes and businesses after a major storm or earthquake.¹⁵ Environmental degradation caused by growing populations with little infrastructure support, no external income and few alternative energy options can lead to increased crisis risk for areas that depend on surrounding and distant ecosystems.¹⁶ For these reasons, security sector resilience should consider climate extremes and changes to the environment, rapid unsustainable urbanization and population displacement (especially undocumented populations in urban slums and refugee camps), emergencies of scarcity and food security (water, food, arable land, natural resources), and biodiversity crises (extinctions, protected reserves, ecosystem health).¹⁷

These stressors in Figure 3 are not direct drivers of crises but risk multipliers that reinforce and exacerbate existing political, socioeconomic tensions and vulnerabilities that destabilize and undermine crisis resilience.¹⁸ Where adaptation to these stressors is

¹⁵ UNISDR, *Disaster Resilience Scorecard for Cities*, UNISDR, *How to Make Cities More Resilient - A Handbook for Local Government Leaders*.

¹⁶ Ibid.

¹⁷ Deon Canyon, Frederick M. Burkle & Rick Speare, "Managing Community Resilience to Climate Extremes, Rapid Unsustainable Urbanization, Emergencies of Scarcity, and Biodiversity Crises by use of a Disaster Risk Reduction Bank," *Disaster Medicine and Public Health Preparedness*, Vol. 9, No. 6(2015), pp. 1-6.

¹⁸ Onita Das, "Climate change and armed conflict: Challenges and opportunities for maintaining international peace and security through climate justice," In R. Abate, *Climate Justice: Case Studies in Global and Regional Governance Challenges* (Washington D.C.: Environmental Law Institute, 2016). Retrieved from <http://eprints.uwe.ac.uk/30412>; Deon Canyon, Frederick M. Burkle & Rick Speare, "Managing Community Resilience to Climate Extremes, Rapid Unsustainable Urbanization, Emergencies of Scarcity, and Biodiversity Crises by Use of a Disaster Risk Reduction Bank."

ineffective, populations will become displaced as they leave for more habitable environments. Such migration often triggers conflict with other communities as competition for dwindling resources escalates.¹⁹ For example, the Syrian drought from 2007 to 2010 helped fuel the Syrian civil war. Widespread crop failure and unemployment caused mass displacement and migration to economically depressed cities, which could not sustain the burden.²⁰ The United Nations Environment Programme (UNEP) highlighted a similar causal link in its 2007 report, "Sudan: Post-conflict Environmental Assessment." Without resilience, such causal links will become worse as we move into a future characterized by a rapidly increasing global population competing for dwindling resources.

The concept of resilience increases the ability of the security sector to prioritize resources and economic stimulus to those most in need before, during and after a crisis. For example, it creates an understanding of community needs and capacities, strengthens relationships with communities, and provides better partnering and coordination with the full spectrum of volunteers and society.²¹ The benefits of this collaborative approach were realized after the Nepal earthquake response when community groups with a relevant work history and experience were more effective in aid distribution than

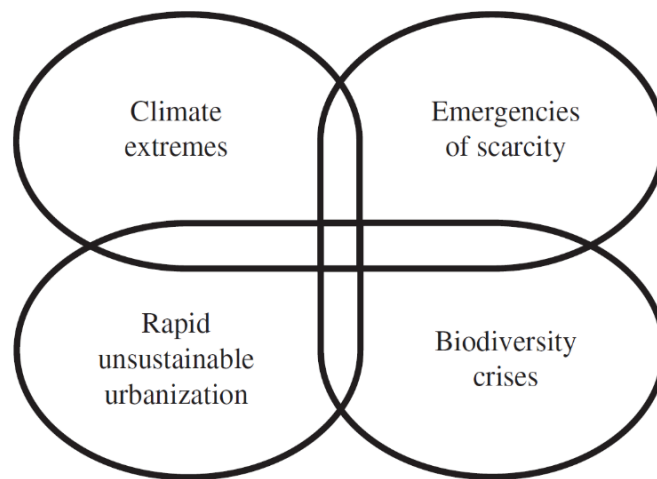
¹⁹ Onita Das, "Climate change and armed conflict: Challenges and opportunities for maintaining international peace and security through climate justice."

²⁰ Ibid.

²¹ U.K. Government, "The context for community resilience," 2016, October 26, Retrieved December 28, 2017, from <https://www.gov.uk/government/publications/community-resilience-framework-for-practitioners/the-context-for-community-resilience#the-benefits-of-resilient-individuals-businesses-and-communities>

inexperienced international actors.²² Furthermore, every US\$1 invested in preparedness not only saves lives, but can save US\$4 in relief and reconstruction costs after a disaster, so resilience is a result of improved economic awareness on the part of those responsible for prioritizing funding streams.²³

Figure 3 - Current and Future Crisis Risks-ecosystem and built environment stressors



Source: Deon Canyon, Frederick M. Burkle & Rick Speare, “Managing Community Resilience to Climate Extremes, Rapid Unsustainable Urbanization, Emergencies of Scarcity, and Biodiversity Crises by use of a Disaster Risk Reduction Bank,” pp. 1-6.

Why Engage at the Local Level?

²² Alistair Cook, Maxim Shrestha & Zin Bo Htet, *The 2015 Nepal Earthquake: Implications for Future International Relief Efforts* (Singapore: RSIS Centre for Non-Traditional Security Studies, 2016).

²³ Multihazard Mitigation Council, *Natural Hazard Mitigation Saves: An Independent Study to Assess the Future Savings From Mitigation Activities - Volume 1: Findings, Conclusions, and Recommendations* (Washington DC: National Institute of Building Sciences, 2005).

The local level is where experiences and perceptions can be drawn on to identify the requirements for effective preparedness, response, recovery and adaptation. Crisis and disaster risk reduction begins and ends at the local level where impacts manifest.²⁴ Local governments in risk-prone areas, including business and informal settlements, become more resilient through empowerment and ownership if engaged to

All levels of government including the security sector need to engage with their communities to improve resilience.

assist in the identification of priorities, risk factors and vulnerabilities. The Indian National Disaster Management has put this concept into action by partnering with Facebook. It provides disaster responders access to maps of affected areas and gets real-time information to people while

providing feedback from those affected through local disaster information volunteers.²⁵

Inclusion of all members of society at a local level is a key requirement for effective resilience. Without this, vulnerable groups with special needs, such as persons with disabilities, may be overlooked.²⁶ An online survey conducted by UNISDR in 2013, involving more than 5,000 people

²⁴ Deon Canyon, Frederick M. Burkle & Rick Speare, "Managing Community Resilience to Climate Extremes, Rapid Unsustainable Urbanization, Emergencies of Scarcity, and Biodiversity Crises by Use of a Disaster Risk Reduction Bank."

²⁵ NDMA, "PRESS RELEASE Kiren Rijju inaugurates NDMA's India Disaster Response Summit," National Informatics Centre, November 9, 2017, Retrieved from <http://pib.nic.in/newsite/PrintRelease.aspx?relid=173344>

²⁶ Marita Vos & Helen Sullivan, "Community Resilience in Crises: Technology and Social Media Enablers," *Human Technology: An Interdisciplinary Journal on Humans in ICT Environments*, Vol. 10, No. 2(2014), pp. 61-67.

with disabilities from 137 countries, found 10% of respondents believe their local government has emergency, disaster management or risk reduction plans that address their access and functional needs, and 20% reported they can independently evacuate immediately without difficulty in the event of a sudden disaster. Also, 51% of respondents expressed a desire to participate in community disaster risk reduction processes.²⁷

Investing in resilience at the local level enhances community spirit, improves economic and social well-being, and fosters greater trust in government from the public and private sectors. This includes: strengthened trust in political structures; reduction in fatalities, serious injuries and property damage; active community participation; protection of assets and cultural heritage; increased investment in infrastructure; business opportunities, as well-governed communities attract investment; and balanced ecosystems to increase availability of fresh water, reduce pollution and food security.²⁸

How to Build and Sustain Resilience?

To build and sustain resilience, a community must have the ability to self-organize and mobilize available resources during and after a crisis.²⁹ This requires interdisciplinary collaboration, which includes amalgamation of organizations beyond the traditional disaster and crisis management system (government agency focus) to allow educational, community and private organizations such as universities,

²⁷ UNISDR, *Disaster Resilience Scorecard for Cities*, UNISDR, *How to Make Cities More Resilient - A Handbook for Local Government Leaders*.

²⁸ Ibid.

²⁹ Marita Vos & Helen Sullivan, "Community Resilience in Crises: Technology and Social Media Enablers."

primary health care sector (general practitioners and pharmacies) and transport companies to help manage the problem.³⁰ Using interdisciplinary collaboration, the economic and security sectors can lead articulation and operational discussions on the need to achieve crisis resilience to governmental decision makers, the community, businesses and non-government organizations. For example, after the Indian Ocean tsunami in 2004, the level of devastation in Aceh Province, Indonesia extended well beyond the capacity of the disaster management agency. This led to the creation of a rehabilitation and reconstruction agency that formed partnerships between communities, the private sector and local authorities to allow all stakeholders to be involved in the recovery process. This approach greatly improved coordination and accelerated the reconstruction process.³¹

Effective resilience requires strong ecosystems and built environments, such as health services, transport infrastructure, the electrical grid, water quality, sanitation systems and other municipal utilities required to protect and preserve the health and well-being of communities.³² Social support systems such as neighborhoods, family and kinship networks, social cohesion, mutual interest groups and mutual self-help

³⁰ Benjamin J. Ryan, Richard C. Franklin, Frederick M. Burkle, Erin C. Smith, Peter Aitken, Kerrianne Watt, Peter A. Leggat, "Ranking and prioritizing strategies for reducing mortality and morbidity from noncommunicable diseases post disaster: An Australian perspective," *International Journal of Disaster Risk Reduction*, Vol, 27 (2018), pp. 223-238.

³¹ UNISDR, *Disaster Resilience Scorecard for Cities*, UNISDR, *How to Make Cities More Resilient - A Handbook for Local Government Leaders*.

³² Deon Canyon, Frederick M. Burkle & Rick Speare, "Managing Community Resilience to Climate Extremes, Rapid Unsustainable Urbanization, Emergencies of Scarcity, and Biodiversity Crises by Use of a Disaster Risk Reduction Bank."

groups are important for building resilience.³³ To mitigate this risk, all levels of government including the security sector need to engage with their communities to improve resilience.

An increasingly common methodology used to build resilience is the UNISDR's "Ten Essentials for Making Cities Resilient." Although focused on cities, this approach is relevant at the local government level because it covers many common issues that need to be addressed to improve resilience. In Table 1 below, Essentials 1-3 cover governance and financial capacity; 4-8 cover the dimensions of planning and disaster preparation; and 9-10 cover the disaster response and post-event recovery.

Table 1 – The Ten Essentials for Making Cities Resilient

Essential	Activities
1. Organize for disaster resilience	Put in place an organizational structure with strong leadership and clarity of coordination and responsibilities. Establish Disaster Risk Reduction as a key consideration throughout the City Vision or Strategic Plan.
2. Identify, understand, and use current and future risk scenarios	Maintain up-to-date data on hazards and vulnerabilities. Prepare risk assessments based on participatory processes and use these as the basis for urban development of the city and its long-term planning goals.

³³ Paul Arbon, Lynette Cusack, Kristine Gebbie, Malinda Steenkamp & Olga Anikeeva, *How do we measure and building resilience against disaster in communities and households* (Adelaide, Australia: Torrens Resilience Institute, 2013).

3. Strengthen financial capacity for resilience	Prepare a financial plan by understanding and assessing the significant economic impacts of disasters. Identify and develop financial mechanisms to support resilience activities.
4. Pursue resilient urban development and design.	Carry out risk-informed urban planning and development based on up-to-date risk assessments with particular focus on vulnerable populations. Apply and enforce realistic, risk compliant building regulations.
5. Safeguard natural buffers to enhance the protective functions offered by natural ecosystems	Identify, protect and monitor natural ecosystems within and outside the city geography and enhance their use for risk reduction.
6. Strengthen institutional capacity for resilience	Understand institutional capacity for risk reduction including those of governmental organizations; private sector; academia, professional and civil society organizations, to help detect and strengthen gaps in resilience capacity.
7. Understand and strengthen societal capacity for resilience	Identify and strengthen social connectedness and culture of mutual help through community and government initiatives and multimedia channels of communication.
8. Increase infrastructure resilience	Develop a strategy for the protection, update and maintenance of critical infrastructure. Develop risk mitigating infrastructure where needed.
9. Ensure effective preparedness and disaster response	Create and regularly update preparedness plans, connect with early warning systems and increase emergency and management capacities. After any disaster, ensure that the needs of the affected

	population sit at the center of reconstruction, with support for them and their community organizations to design and help implement responses, including rebuilding homes and livelihoods.
10. Expedite recovery and build back better	Establish post-disaster recovery, rehabilitation, and reconstruction strategies that align with long-term planning and providing an improved city environment.

Source: UNISDR, *Disaster Resilience Scorecard for Cities* (Geneva: United Nations Office for Disaster Risk Reduction, 2017).

To drive action, UNISDR developed a “Disaster Resilience Scorecard for Cities” based on the “Ten Essentials for Making Cities Resilient”. This scorecard provides an assessment that allows local governments to monitor and review progress and challenges in the implementation of the Sendai Framework for Disaster Risk Reduction – 2015-2030, and assess their level of disaster resilience.³⁴ The guide shows how to achieve optimal resilience, and challenges complacency by reminding authorities and stakeholders that there is always more to be done to build and sustain resilience. Essentials 1 to 3 are intended to be accomplished first, while the remaining essentials may be completed in any order. Scoring occurs at two levels:

Level 1: Preliminary level, responding to key Sendai Framework targets and indicators, and with some critical sub-questions. This approach is for use in a 1 to 2 day city multi-stakeholder

³⁴ UNISDR, *Disaster Resilience Scorecard for Cities*; UNISDR, *How to Make Cities More Resilient - A Handbook for Local Government Leaders*.

workshop. In total there are 47 questions indicators, each with a 0 to 3 score.

Level 2: Detailed assessment. This approach is a multi-stakeholder exercise that may take 1 to 4 months and can be a basis for a detailed city resilience action plan. The detailed assessment includes 117 indicator criteria, each with a score of 0 to 5.

Recommendations to Enhance Political, Economic and Social Stability

I . Security Sector Scorecard

A security sector resilience scorecard should be developed to provide a mechanism for measuring stability. The UNISDR's "Ten Essentials for Making Cities Resilient" provides a template for developing such a scorecard. Thematical areas of focus could include the underlying risk drivers of societal collapse from a crisis such as poverty and inequality, poor living conditions, unplanned urbanization processes, ecosystem and built environment stressors, and lack of regulations and enforcement.³⁵

Development of the scorecard should be led by a team of multi-disciplinary security experts and crisis scholars with experience in the Indo-Pacific. This would enable the region to better prepare for and respond to crises by helping to understand the risk of disasters and the need for political, economic and social resilience. Multi-sectoral participation, including private sector partnerships, will improve

³⁵ UNISDR, *Implementation guide for local disaster risk reduction and resilience strategies - Public consultation version* (Geneva: United Nations Office for Disaster Risk Reduction, 2018).

collaboration on crisis preparedness issues and strengthen regional capacity to mitigate, prepare, respond and recover from crises.

Completion of the scorecard should be led by local governments with support from security experts, non-government organizations, community members and provincial, national government and regional agencies. It could be mandated at local, provincial and/or national levels through legislation, financial incentives or regional agreements. If developed and implemented, a community-focused scorecard aggregated across local, provincial, national and regional levels would provide a systems-based approach to understanding security sector risks and priority areas for enhancing resilience across the Indo-Pacific.

II . Cluster Approach to Resilience and Stability

A cluster approach to resilience is recommended to systematize the management of building and sustaining political, economic and social stability. This concept derives from the U.N. Cluster Approach to humanitarian and disaster response, which includes U.N. and non-UN organizations that focus on different sectors of humanitarian action (e.g. water, health and logistics) during the time of a disaster or crisis.³⁶

If resilience is weak or does not exist, a crisis acts as a negative multiplier that reinforces and exacerbates existing political, socioeconomic tensions.

³⁶ OCHA, "Cluster Coordination," United Nations Office for the Coordination of Humanitarian Affairs, May 10, 2018, Retrieved from <http://www.unocha.org/legacy/what-we-do/coordination-tools/cluster-coordination>

Adoption of this type of proven and field-tested approach would provide a well-rounded mechanism and decision-making tool for enhancing political, economic and social resilience.

Due to the range of disciplines involved in achieving resilience, development and implementation of a “Cluster Approach to Resilience and Stability” will require collaborative governance.³⁷ This would start with multi-disciplinary security experts and crisis scholars articulating the need to measure, build and sustain political, economic and social resilience (incentive to participate).³⁸ The next steps would be: face-to-face discussions; trust building to develop a shared understanding; engaging in comprehensive and shared planning; pooling and jointly acquiring resources; and achieving intermediate outcomes such as agreeing on the need for resilience.³⁹ Through this approach an open, inclusive and constructive dialogue would occur, to create shared values for achieving resilience. This will provide the foundation for a well-rounded decision-making framework to develop a “Cluster Approach to Resilience and Stability” that builds and sustains political, economic and social stability across the Indo-Pacific.

Conclusion

³⁷ Janine O'Flynn & John Wanna, *Collaborative Governance: A new era of public policy in Australia?* (Canberra: ANU Press, 2008); Benjamin Ryan et al. “Ranking and prioritizing strategies for reducing mortality and morbidity from noncommunicable diseases post disaster: An Australian perspective.”

³⁸ Chris Ansell & Alison Gash, “Collaborative governance in theory and practice,” *Journal of Public Administration Research and Theory*, Vol. 18, No. 4 (2008), pp. 543-571; John Donahue, “On Collaborative Governance,” *Corporate Social Responsibility Initiative Working Paper No.2* (Cambridge, MA: John Kennedy School of Government, Harvard University, 2004).

³⁹ Ibid.

Crisis resilience has a critical role in building and sustaining political, economic and social stability across the Indo-Pacific. This must be understood by the security sector due to the increasing complexity, and the often multidisciplinary and transboundary nature, of modern-day crises. If resilience is weak or does not exist, a crisis acts as a negative multiplier that reinforces and exacerbates existing political, socioeconomic tensions and vulnerabilities that can have a destabilizing affect and result in societal collapse. To prevent this from occurring, a security sector resilience scorecard must be developed to measure and help build and sustain stability. Implementation would enable the region to better prepare for and respond to crises by helping to understand risks and identify priority areas for action. This scorecard would need to be complemented by a Cluster Approach to Resilience and Stability to systematize the management of building and sustaining political, economic and social stability. Achieving this will provide a well-rounded and systems-based approach to enhancing local, provincial and national level crisis resilience and stability across the Indo-Pacific.

(The views expressed in this article are those of the authors and do not necessarily reflect the official policy or position of the Daniel K. Inouye Asia-Pacific Center for Security Studies, the Department of Defense, or the U.S. Government.)

***Dr Benjamin J. Ryan** is an Associate Professor of Daniel K. Inouye Asia-Pacific Center for Security Studies, Honolulu HI, USA. **Dr. Deon V. Canyon** and **Dr. James Campbell** are Professors of Daniel K. Inouye Asia-Pacific Center for Security Studies. **Dr. Frederick M. Burkle, Jr.** is a Senior HHI Fellow of Harvard Humanitarian Initiative, Visiting Scientist of Harvard School of Public Health, and Professor of the Department of Community Emergency Health of Monash University Medical School. **Dr. Wie-Sen Li** is an Executive Secretary of the National Science and Technology Center for Disaster Reduction, Taiwan.*

Reflections on The Rise of China's Navy

By James Goldrick

China's powerful new warships have attracted much coverage in the global media in recent years. Far less attention has been devoted to the evolution of the strategic culture which must underpin the country's drive to develop a first-class navy. The changes will need to be profound. Despite China's navalists' attempt to summon history to their aid with narratives of the treasure voyages of Admiral Zheng He in South East Asia and the Indian Ocean, China's outlook has been fundamentally continentalist over practically its entire history. External economic engagement through the Silk Road and maritime South East Asia was beneficial, but never existential. China's economy was self-sustaining and its primary security interests – and threats – usually related to its northern and western borders. This was an outlook that successive governments found impossible to change. Largely because of this rigidity, the century of western and Japanese intervention from the sea was marked by China's repeated failures to make an effective maritime response.

China must now balance its continental concerns, which remain extant (and complex), with the requirements imposed by a new dependence on the maritime domain. China's recent history means that it will always have an eye on the need to protect itself against attack from the sea, but there is much more to China's vulnerability than potential invasion or bombardment. Most of China's global trade moves by sea. The realities of transport costs mean this will remain the case no matter how

successful the “Belt” element of its grand economic plan may be. Furthermore, China is critically dependent on the seaborne import of raw materials, notably energy, from Middle East oil to liquefied natural gas. Finally, China’s global engagement, particularly in Africa and the Middle East requires regard for the safety of its nationals in unstable regions as well as protection of its investments. The “One Child” policy has created a concern for the well-being of individuals that may be new to China’s government but has certainly been evident in its readiness to conduct evacuation operations as far away as the Mediterranean and cooperate in the search for the lost MH 370 flight in the Indian Ocean.



Taiwan’s indigenous stealthy Tuo Chiang class missile corvettes conducting sea trials. (Source: Military News Agency)

At the same time, China’s concerns for its hinterland have not diminished. Its security is dependent upon the stability of the many states with which it shares borders and on achieving sufficient economic growth in its western provinces. Neither the security problems nor the economic challenges involved will be easy to resolve. The recent

tensions with India over the two nations' territorial claims are just one example of the difficulties which can arise, sometimes with little notice.

All this is not new and Chinese naval strategists have been looking hard at the work of the nineteenth century navalist and geo-strategist Alfred Thayer Mahan. He is famed for analysing the elements of British sea power and its contribution to Britain's rise to global dominance. Mahan, however, was interested in not only why an island nation such as Britain should develop in such a way, but why its greatest rival, France, did not. France, a continental power as well as a maritime one, had to balance its efforts between the land and the sea in a way that Britain did not, and Mahan had much to say about the nature of its failure to do so.

The lesson of France is important because China's strategic planners must attempt to ride the two horses of continental defence and protection and assertion of its maritime interests. In the maritime domain, this is reflected in the parallel efforts to develop a force structure on one hand capable of preventing enemy forces from approaching China by sea and on the other able to conduct classical sea control and power projection force across the wider region – and even globally. If the resources continue to flow, the Chinese People's Liberation Army Navy (PLA-N) will aim for surety that it can dominate the maritime approaches to China, a task that will be managed in conjunction with the other arms of the PLA, such as the air force and the rocket force. It will continue to develop fast, missile equipped coastal surface craft, as well as diesel-electric submarines. Emergent technology, not only in anti-ship cruise and ballistic missiles, but in the form of unmanned surveillance and attack vehicles will be a key element of this effort, as will be long range and space-based sensors. Ironically, China's "asymmetric" efforts to create an "anti-access, area denial" capability in the western Pacific will rely upon much the same systems

of such sensors and long-range communications that the United States has developed over the last century to support its own operations. The truth is that a Sino-US conflict in the western Pacific would be as much a contest between and against networks as one of purely kinetic effects.

For Taiwan, the irony may lie in the fact that the desire to deploy China's naval power in distant seas rather than the need for coastal defence is making the mainland look at the island in a new way. Until this point, the default Chinese military attitude, understandable in the wake of the "century of shame", has been to possess the ability to deter and defeat any would-be seaborne invader. Now China is looking to the sea as its access to the globe, reunification will have a new urgency. Control of Taiwan would give China passage to deep water and the Pacific Ocean without the need to transit through waters under the surveillance of other powers.

Artificial island building in the South China Sea reflects both continentalist and maritime thinking, but it is possible their mixture will go too far in the eyes of the region. The danger is that the continentalists who genuinely regard the new installations as being a "Great Wall at sea" for China's defence will make the mistake of thinking that the seas that lie between them and the mainland are Chinese territory. If this assumption is taken to its logical conclusion by attempting to eject other nations from commercial or military operations within the area encompassed by the "Nine Dashed Line", the consequences for China's relationship with the other states bounding the South China Sea would be disastrous, however strong China's historic claims to its islands and features may be. This would also have profound implications for the way that China is regarded in the wider region and, arguably, globally.

The reality is that this step is unnecessary. The military intent of achieving a much greater level of awareness across the sea by setting up the artificial islands as surveillance platforms and bases for surface and air assets is well on its way to being achieved. In a high intensity conflict, the “unsinkable aircraft carriers” may well become “immovable targets”, but their utility in a wide range of contingencies, as forward bases for long range operations and as very public statements of China’s growing

Control of Taiwan would give China passage to deep water and the Pacific Ocean without the need to transit through waters under the surveillance of other powers.

maritime power is undeniable. This is not the only case in which China’s maritime thinkers have the challenge of developing within the national policy-making elite an understanding of just how the sea is different from the land, but it is probably the most important.

An associated challenge is the need to be sensitive to the reactions of other nations in the employment of maritime power. For a country which

sees itself as the historical victim of the aggressive use of naval power, China has on occasion been surprisingly obtuse in its employment of its new capabilities. Publicly justifying the deployment of submarines into the Indian Ocean under the flimsy pretext of anti-piracy operations not only alienated India but also took away much of the credit associated with the long running surface deployments which have significantly assisted the international effort to suppress piracy in the western Indian Ocean. Similarly, while China has made much of its view that foreign intelligence gathering operations are illegal within its Exclusive Economic Zone (EEZ), this has not stopped the PLA-N dispatching its own intelligence ships into other nations’ EEZs. The PLA-N also missed

some early opportunities to prove itself in disaster relief, notably when the Philippines were hit by tornadoes, although its recent deployment of a hospital ship to the South Pacific suggests the lesson is beginning to be learned.

The level at which the force structure of the PLA-N finally settles remains an open question. A rule of thumb may be that China would like to possess, with comparable levels of weapons and sensors in its major combatant ships, a front-line navy approximately half the size of the U.S. Navy (USN). In achieving such a goal, much will depend, as sustained naval development always does, on the ability of China's economy to support the expanding needs of its new navy. As it acquires so many sophisticated capabilities, the PLA-N must come to terms with the scale of the overheads involved and this may cause intense budgetary conflicts within the PLA as well as the government as a whole. The real costs of naval power do not lie in ship construction, but in operation and sustainment over the long term and this must be increasingly apparent to senior decision makers. The aircraft carrier program alone requires not only a network of air bases ashore, together with the design and manufacture of naval aircraft, but also a support system that will allow China's carrier groups to conduct protracted operations at long range. The new 45,000-ton fast replenishment ship which was commissioned in 2017 is just one element of the matrix of capabilities that will be needed. Even providing spare parts at short notice becomes a highly resource-intensive operation when it is conducted at oceanic distances. This may be one factor in the apparent change of attitude to overseas bases on the part of the Chinese government. Even with expensive facilities such as that being developed in Djibouti, however, the PLA-N will have to pour much more money into its fleet train if it is to sustain forward deployed forces at the appropriate levels.

Despite such realities, development of the carrier force will continue as a pillar of the PLA-N's intended power projection capabilities. The Chinese carriers should be regarded as emulation of American capabilities to achieve strategic effects rather than a direct military challenge to the USN. They are part of China's competition with the United States, but they will not be critical to any conflict with the Americans. The PLA-N will understand Chinese naval aviation is a very small child by comparison with the American effort. But it is also aware that its carrier battle groups will be a formidable proposition for anyone else and thus potentially an important tool for strengthening China's strategic position within the region. It will not have escaped the PLA-N that carriers have a wide utility in addition to the projection of power. The USN response to the 2004 tsunami, which saw 25 ships assigned to help the affected areas in South East Asia within ten days, is a good example. Amongst those units was an aircraft carrier, whose ability to function as a mobile airfield was critical to the provision of aid to remote areas.

A key test for the PLA-N will be the success of the second indigenous-built carrier. The first unit, allegedly named Shandong, whose trials started earlier in 2018, is largely based on the Liaoning and shares the limitations of that ship's lack of catapults. The second unit will be a Chinese design from the keel up. Whether it employs steam catapults or the electromagnetic systems which the USN is having so much trouble bringing into service in its latest carrier, the new ship will take much longer to build than Shandong and even longer to bring to an operational level of capability. Its design inevitably carries much greater risks than the modification of the eight truck-loads of plans which came with the Liaoning that resulted in the Shandong. If the new Chinese design proves successful, however, the carrier force is likely to round out at six units by the early 2030s. This would provide the capability to

have one battle group deployed in distant waters at all times, plus the ability to surge to two such deployments for a significant period. The principal operating area for the deployed carrier will almost certainly be the Indian Ocean, but the recent history of Chinese deployments to northern Europe and other parts of the world suggests that the PLA-N will occasionally send a group much further afield. This may even include the Caribbean if China wishes to push home to the United States the message of its potential global reach. Such a message, albeit only using destroyers and frigates, has already been given to northern Europe with a task group deployment to the Baltic and associated Sino-Russian naval exercises.

A capable nuclear attack submarine force will be an important contribution to sea control and power projection, as well as possessing significant potential to support continental defence.

The force of major surface combatants will probably remain at the present number of 70 to 80, but with a very different size and capability mix. At its summit by 2030 will be up to a dozen of the new Type 055 cruisers – a much more accurate label for their size and role than destroyers – with the remainder being made up of a mix of air warfare destroyers and anti-submarine frigates. Both destroyers and frigates will possess significant general capabilities in addition to their specialist role. The PLA-N seems to have learned the lesson that over-specialisation limits the flexibility with which units can be employed in unexpected contingencies.

The amphibious force will continue to expand to provide up to six expeditionary groups to allow similar deployment patterns to the carriers – at least one group always available for deployment and the

ability to surge to a second. The recent decision to expand China's marines confirms the PLA's interest in developing its long-range intervention capabilities, although the existence of Taiwan will be an important factor in the continuing development of platforms and landing forces which have utility closer to home.

There will be a price to pay. At a time when the USN is facing many problems, despite its mature force structure, the PLA-N has its own challenges. Developing a full range of contemporary force elements to their full potential is and will not be that easy, particularly as the Chinese have few external sources of support. The Russians can help (for a price) in some areas, but they have their own strategic agendas and will be loath to provide China with the latest technologies in which they have maintained a lead. No matter how closely the PLA-N has watched the way that the USN works, meeting the requirements involved in putting in place, manning and financing the constellation of tactical development, experimentation, doctrine writing, training, and maintenance organisations that are needed to keep a great power navy running will be a huge challenge. The effort will certainly be critically dependent on the continuing ability of the government to pay for it. If China's economic growth stalls, then it is likely that the sea control and power projection effort will be an early victim.

The fitful progress of the submarine arm is a good example of the problems the PLA-N must be facing. Neither the nuclear ballistic missile submarine, nor the nuclear attack submarine program have progressed quickly. While the US Department of Defense has for some years assessed the Jin class SSBN as constituting "China's first credible, sea-based deterrent", only four units are yet operational. Other nations have maintained continuous underwater deterrent patrols with only four units, but the PLA-N at its present state of expertise would require at

least five and preferably six boats to be sure of maintaining such an effort.



PLA Navy Type 054A frigate 515 Binzhou operating into west Pacific in October 2018. (Source: Japan Ministry of Defense)

Similarly, the PLA-N has only five operational nuclear attack submarines, nearly 45 years after the first such unit commissioned. More are under construction and the operational employment of these units has been much more ambitious in the last few years, including deployments to the Indian Ocean. The submariners are clearly eager to gain experience in other environments than the littoral of China. Nevertheless, the scale of the nuclear attack submarine (SSN) building programme so far compares oddly with the effort devoted to surface forces. It suggests that China is still struggling with the quality of its nuclear power plants and the associated noise levels, as well as many other elements of submarine design and construction. Much has been claimed by the PLA-N in recent months about the technological breakthroughs which have been achieved by Chinese scientists and engineers and this may well be the case. Indeed, the apparently slow progress with the submarine fleet could be because the PLA-N is furiously trialling new systems and technologies with the aim of embarking on new large-scale building programmes only when it can be sure that the necessary technical advances have been achieved. A capable nuclear attack submarine force will be an important

contribution to sea control and power projection, as well as possessing significant potential to support continental defence. Both the carrier groups and the missile submarines will want the protection and support of accompanying SSNs. The PLA-N's target is likely to be 25 or more boats, but this may take even longer to achieve than a mature carrier force.

In sum, China has achieved extraordinary advances in naval capability in the past decade. The PLA-N cannot yet claim supremacy in either its defensive mission or its power projection efforts and the realities of the strategic situation mean that it may never be able to do so. Even aside from the United States, nations such as Japan wield formidable capabilities at sea. The PLA-N still has much to put in place and much to learn before its new force elements can be considered mature and remains vulnerable to the limits on its budget that may result from an economic downturn or the assertion of the interests of other elements of the PLA who do not give the maritime domain the same priority. Above all, if it is to make a constructive contribution to China's rise as a global power, China's navy needs to understand the full meaning of the words of an American president spoken at the outset of the growth of American naval power and learn to speak softly, even when carrying a big stick.

∞

Professor James Goldrick is an Adjunct Professor in the Strategic and Defence Studies Centre of The Australian National University and School of Humanities and Social Sciences in the University of New South Wales at the Australian Defence Force Academy. Professor Goldrick was a senior officer in the Royal Australian Navy until he retired in 2012. He is a Nonresident Fellow at the Lowy Institute. His books cover naval history and maritime strategy.

∞

The United States Seventh Fleet Patrol and Taiwan: Past and Present

By Catherine Kai-ping Lin

The US sent two destroyers through the Taiwan Strait on July 7 and a cruiser and a destroyer on October 22, 2018,¹ to underscore the US resolve in the trade war against the People's Republic of China (PRC) and to show the US determination to defend the freedom of navigation not only in the Taiwan Strait but also in the South China Sea. Two destroyers patrolling down the Taiwan Strait in fact already constituted the regular US Seventh Fleet patrol of the Taiwan Strait from 1950 to 1969, known as the Taiwan Patrol Force (TPF). This article will describe briefly what the Seventh Fleet's TPF in the Taiwan Strait was and try to place the patrol in the contemporary context.

¹ Ryan Browne, "US Destroyers Sailed through Taiwan Strait," *CNN*, July 21, 2018, <https://edition.cnn.com/2018/07/07/politics/taiwan-strait-us-ships/index.html>; Ryan Browne and Barbara Starr, "US Sails Warships through Taiwan Strait amid Tensions with China," *CNN*, October 23, 2018 <https://edition.cnn.com/2018/10/22/politics/us-warships-taiwan-strait-china/index.html>; the US in fact just sent a destroyer and a replenishment oiler through the Taiwan Strait on November 28, 2018, as this article was about to go off to print, Ben Werner, "U.S. Guided-Missile Destroyer, Oiler Transit Taiwan Strait," *US Naval Institute News*, November 28, 2018, <https://news.usni.org/2018/11/28/39>

The Establishment and Termination of the Taiwan Patrol Force ²

The Chinese Nationalists (Kuomintang) after losing the Chinese civil war to the Chinese Communists in 1949, under the assistance of the US Navy, retreated to Taiwan. At this time, the Chinese Nationalists still held twenty to thirty small islands along the southeastern coast of China. The Chinese Communists wanted to take over those offshore small islands, and the Chinese Nationalists still wanted to fight back and re-take the mainland. As a result, holding on to those small islands became important to the Chinese Nationalists. Many had also predicted that the Chinese Communists were highly likely to attack Taiwan in the summer of 1950.

However, the Korean War broke out on June 25, 1950. The US President Harry Truman, who was about to give up on Chiang Kai-shek (CKS),³ had no choice but to announce a “neutralization” plan for the Taiwan Strait on the one hand to protect Taiwan from being seized by the Chinese Communists, and on the other hand to prevent CKS from counterattacking mainland China.⁴ On August 4, 1950, the US Seventh Fleet established Task Group 77.3, which would eventually evolve into

² This and the next two sections are primarily based on material from Bruce A. Elleman's *High Seas Buffer: The Taiwan Patrol Force, 1950-1979* (Newport, Rhode Island: Naval War College Press, 2012) and *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy* (Lanham, MD: Rowman & Littlefield, 2015).

³ Chiang Kai-shek was the president of the Republic of China (ROC) on Taiwan and thus the leader of the Chinese Nationalists after the Korean War broke out. Website of the Office of the President of the Republic of China (Taiwan), <https://www.president.gov.tw/Page/83>

⁴ Nancy Bernkopf Tucker, *Taiwan, Hong Kong, and the United States, 1945-1992: Uncertain Friendship* (New York: Twayne Publishers, 1994), pp. 32-33.

the TPF, and the surface component became TG 72.1, surveilling and guarding the sea and air spaces of the Taiwan Strait, as well as keeping tensions in the Taiwan Strait from escalating into war.

The TPF at first constituted included an average of four destroyers in or near the Taiwan Strait at any one time and covered the area from the East China Sea through the strait down to the South China Sea.⁵ “A typical patrol in the Taiwan Strait might begin in waters just south of Japan; a ship would pass the Penghu Islands and then cruise by southern Taiwan. Meanwhile, other ships were usually patrolling in the opposite direction, heading north.”⁶ If four ships were assigned to the TPF, the ships could rotate on patrol, alternately spending five days on patrol and five days in port.⁷ When the Vietnam War heated up in the 1960s, “the destroyers, with their five-inch guns, were required there for shore bombardment duties.”⁸ Consequently, smaller destroyer escorts (or DERs), meant for radar picket duty, were assigned to the TPF patrol. Their three-inch guns were less suitable for the shore bombardment role in Vietnam.⁹ During slack periods, two DERs, rather than four destroyers, would be on assignment. “The usual operating pattern for two ships was one at sea for a week, while the other was on call in either Kaohsiung or Keelung; turnovers were normally conducted at sea.”¹⁰ According to Bruce A. Elleman, Taiwan Strait provided excellent training for the US Navy, “since the weather conditions there were some of the worst in their naval experience,”¹¹ and “during the 1950s, the need to

⁵ Elleman, *High Seas Buffer: The Taiwan Patrol Force, 1950-1979*, p. 20.

⁶ *Ibid.*, p. 28.

⁷ *Ibid.*, p. 21.

⁸ *Ibid.*, p. 22.

⁹ *Ibid.*

¹⁰ *Ibid.*, p. 23.

¹¹ *Ibid.*, p. 26.

maintain a constant patrol in the Taiwan Strait impacted almost every ship in the US Navy.”¹²



Ships with the Ronald Reagan Carrier Strike Group and John C. Stennis Carrier Strike Group transit the Philippine Sea on November 16, 2018. (Source: U.S. Indo-Pacific Command)

Besides patrolling the Taiwan Strait, in the beginning the Seventh Fleet also worked with the Chinese Nationalists on executing naval blockade along the southeastern coast of China to hinder the maritime trade of the PRC. The US in fact adopted a full embargo on strategic goods on the PRC from December 8, 1950, to June 10, 1971.¹³ During the Vietnam War, the patrolling range of the Seventh Fleet was extended southward to Vietnam.

¹² Ibid., p. 28.

¹³ Ibid., p. 118.

According to Elleman, the TPF played a decisive role in the three Taiwan Strait Crises (1954-55, 1958, and 1962) before the termination of the regular patrol in 1969. The three Taiwan Strait crises to different degrees involved the many offshore islands controlled by the Chinese Nationalists. However, the US neutralization order restricted the Seventh Fleet vessels from participating in the defense of any coastal islands held by the Chinese Nationalists, and the Seventh Fleet would also not interfere with the Chinese Nationalist operations from the coastal islands.¹⁴ Nevertheless, no matter how the US administrations debated throughout the three crises whether to defend or force CKS to give up the offshore islands, the presence of the Seventh Fleet prevented the crises from escalating into all-out wars.

The PRC and the USSR split in the 1960s, and consequently throughout the 1960s the PRC shifted its trading focus from the USSR to Western countries. In 1969, once Richard Nixon became the US president, Nixon and his assistant for national security affairs, Henry Kissinger, decided to seize the moment to restart the on-and-off Warsaw talks, in an effort to balance off the USSR. In exchange for the PRC's positive responses, Nixon-Kissinger terminated the regular patrol of the Seventh Fleet on November 15, 1969.¹⁵ The official US Navy explanation was that the decision was necessary because it was "part of over 100 ship reduction in world-wide US naval deployment, made pursuant to recent \$3 billion reduction in defense expenditures."¹⁶ In trying to assuage CKS, the US

¹⁴ Ibid., p. 60.

¹⁵ Ibid., pp. 117-118.

¹⁶ *Foreign Relations of the United States, 1969-1976, Volume XVII, China, 1969-1972*, ed. Steven E. Phillips (Washington: Government Printing Office, 2006), Document 34.

government further emphasized that the patrol had been only one aspect of the presence of the Seventh Fleet in the strait, that other aspects such as rest and recreation visits and periodic calls by Commander Seventh Fleet would continue, and that whatever additional units of the Seventh Fleet were necessary to fulfill the US commitments under the US-Taiwan Mutual Defense Treaty signed in 1954 were available for immediate deployment to the Taiwan Strait area.¹⁷ The US government further assured CKS that there would be “a material increase in the aggregate number of transits of the Strait per month by ships of the Seventh Fleet. Most of the vessels of the Fleet moving in a north/south direction would transit the Strait rather than travel along the East Coast of Taiwan. As a result, there would probably be more actual transits of the Strait by Seventh Fleet vessels, and a more thorough naval observation of the Strait under the new procedure than when the two DE’s were on regular patrol.”¹⁸ All of the above intermittent activities of the Seventh Fleet involving Taiwan eventually ended on January 1, 1979, as the US and the PRC established formal diplomatic relations.

The Military, Economic, and Political Impact of the Taiwan Patrol Force

The Seventh Fleet’s TPF in the Taiwan Strait exerted enormous impact on US-ROC-PRC relations during the patrol’s existence, as outlined by Elleman. According to Elleman, militarily, due to the TPF, “neither the PRC nor the ROC ever mounted a major attack across the Taiwan

¹⁷ Ibid.

¹⁸ *Foreign Relations of the United States, 1969–1976, Volume XVII, China, 1969–1972*, ed. Steven E. Phillips (Washington: Government Printing Office, 2006), Document 52.

Strait.”¹⁹ This objective remained important, since all attempts to urge a peace agreement on the ROC and PRC failed. The TPF also “acted much like a vernier switch, allowing the US Navy to increase or decrease cross-

The Seventh Fleet’s patrol was also used by the US State Department as a political tool to influence the PRC’s behavior.

strait tensions to suit the US government’s larger policy objectives.”²⁰

The TPF moreover reassured “America’s East Asian allies-- including Japan, South Korea, the Philippines, and Australia-- that the PRC could not invade the First Island Chain.”²¹ The US government at the same time provided the Chinese Nationalists with “a dependable source of military equipment and training to

defend themselves, even while not giving them sufficiently advanced equipment to allow Taiwan to attack the PRC of its own volition.”²² As a result, “the Taiwan Patrol Force also contributed to high morale in Taiwan.”²³

Economically, after the outbreak of the Korean War, the US government adopted a full embargo on strategic goods on the PRC, and the Seventh

¹⁹ Elleman, *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy*, p. 150.

²⁰ Ibid.

²¹ Ibid. According to Elleman, the First Island Chain, “in PRC geostrategic theory, stretches from the Aleutian Islands through the Kurile Islands, the main islands of Japan, the Ryukyu Archipelago, Taiwan, and the Philippines to the Greater Sunda Island.” Elleman, *High Seas Buffer: The Taiwan Patrol Force, 1950-1979*, p. 134; Robert D. Kaplan, “The Geography of Chinese Power: How Far Can Beijing Reach on Land and at Sea?” *Foreign Affairs*, Vol. 89, no. 3 (May/June 2010), p. 33.

²² Elleman, *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy*, p. 151.

²³ Ibid.

Fleet helped execute the embargo and naval blockade with the Chinese Nationalists. Elleman argued that “Washington’s long-range goal was to deny the PRC a wider range of trade partners. Over time, it was hoped that this would add additional friction to the already tense Sino-Soviet relations”²⁴ as the PRC became increasingly dependent on the USSR economically. By the late 1950s, the PRC’s “debts to the USSR had grown to almost \$2 billion, roughly equal to the US government’s economic aid to Taiwan between 1950 and 1969.”²⁵ Mao Zedong, in order to begin to pay off the PRC’s enormous debts to the USSR, adopted economic policies that, such as the Great Leap Forward, generated nationwide famine. Therefore, according to Elleman, the Chinese Nationalist naval blockade and American strategic embargo were “highly successful in furthering the Sino-Soviet rift.”²⁶ On the other hand, although political rights were negligible in Taiwan, Taiwan was in the process of achieving the economic miracle, which would not have been possible without the security provided by the Seventh Fleet.²⁷

The Seventh Fleet’s patrol was also used by the US State Department as a political tool to influence the PRC’s behavior. As the unfriendly relations between the PRC and USSR in the 1960s culminated into the 1969 Sino-Soviet border disputes, according to Elleman, “the Nixon administration’s 1969 decision to change the Taiwan Patrol Force from a permanent to an intermittent patrol sent a potent signal to Beijing. Although Taiwan was told that this change was due to economic

²⁴ Ibid., p. 153.

²⁵ Ibid.

²⁶ Ibid.

²⁷ Ibid., pp. 153-156.

necessity, it was in fact a political decision.”²⁸ Therefore, this gesture to Beijing, which was largely outside the public view, eventually resulted in the re-opening of the Warsaw Talks, Kissinger and Nixon’s trips to the PRC, the normalization of US-PRC relations, US-PRC cooperation in counterbalancing the USSR, and finally the end of the Cold War.²⁹

The Continuing Strategic Impact of the US Navy in the Taiwan Strait

Although the Seventh Fleet’s patrol in the Taiwan Strait officially ceased operations on January 1, 1979, Elleman argued that the US Navy continued to wield strategic impact in the Taiwan Strait, and one of the examples is provided by the 1995-1996 Taiwan Strait crises, in which the American reaction proved similar to those to the earlier Taiwan Strait crises.³⁰

The PRC conducted ballistic missile tests between July 21 and 28, 1995, in the Taiwan Strait in response to the US government granting of an American visa to Taiwan’s president Lee Teng-hui to visit Cornell University.³¹ From August 15 to 25, 1995, the PRC held military exercises involving about twenty warships and forty aircraft. In November 1995, just prior to Taiwan’s December parliamentary

²⁸ Ibid., pp. 157-158.

²⁹ Ibid., p. 158.

³⁰ Elleman, *High Seas Buffer: The Taiwan Patrol Force, 1950-1979*, p. 129; Elleman, *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy*, pp. 132-133.

³¹ Elleman, *High Seas Buffer: The Taiwan Patrol Force, 1950-1979*, pp. 123-124; Elleman, *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy*, pp. 128-129; James Mann, *About Face: A History of America’s Curious Relationship with China, from Nixon to Clinton* (New York: Alfred A. Knopf, 1999), pp. 328-329.

elections, the People's Liberation Army (PLA) staged "further naval, amphibious, and air-assault operations, near Dongshan Island."³² In response, the US Navy sent the *USS Nimitz* through the Taiwan Strait on December 19, 1995, on its way to the Indian Ocean. According to Elleman, "this was the first time an American aircraft carrier had transited the Taiwan Strait since the late 1970s,"³³ and in many ways, this transit paralleled the June 29, 1950, visit by the carrier *Valley Forge*, "which had helped signal the establishment of the Taiwan Patrol Force."³⁴

US Navy has had 18 unsafe or unprofessional encounters with Chinese military forces in the Pacific since 2016.

From March 8 to 25, 1996, the PRC again conducted ballistic missile exercises and live-fire exercises to correspond with the run-up to Taiwan's first presidential elections under universal suffrage on March 23, 1996.³⁵ In response, the US Navy "dispatched the *USS Independence* aircraft-carrier battle group to the area. Its aircraft were patrolling about 100 miles off of Taiwan. The *USS Nimitz* carrier group was also ordered

³² Elleman, *High Seas Buffer: The Taiwan Patrol Force, 1950-1979*, p. 124; Elleman, *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy*, p. 129.

³³ Elleman, *High Seas Buffer: The Taiwan Patrol Force, 1950-1979*, p. 124; Elleman, *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy*, p. 130.

³⁴ Elleman, *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy*, p. 130.

³⁵ Elleman, *High Seas Buffer: The Taiwan Patrol Force, 1950-1979*, p. 125; Elleman, *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy*, pp. 130-131 ; James Mann, *About Face: A History of America's Curious Relationship with China, from Nixon to Clinton*, pp. 335-338; Patrick Tyler, *A Great Wall: Six Presidents and China: An Investigative History* (New York: PublicAffairs, 1999), pp. 31-36.

to return from the Persian Gulf at high speed. Other naval assets included two Aegis guided-missile cruisers and U.S. Air Force RC-135 Rivet Joint electronic surveillance aircraft.”³⁶ This US Navy’s intervention, according to Elleman, in fact “constituted the largest demonstration of American naval diplomacy against China since the first two Taiwan Strait crises of the 1950s.”³⁷ The strategic rationale was again to neutralize the Taiwan Strait as to not allow a cross-strait invasion, which was much the same as in the 1950s. To Elleman, although *Independence* and *Nimitz* were not a new official TPF, they carried out similar functions in the spirit of the Seventh Fleet during the Cold War period.³⁸

The US Seventh Fleet’s Patrol in the Context of the Contemporary US-PRC Strategic Competition/Cold War

Tensions have risen between the US and PRC ever since Xi Jinping assumed the presidency in the PRC in 2012 and unveiled the Belt and Road Initiative in 2013. Since Taiwan’s Democratic Progressive Party’s Tsai Ing-wen became president in 2016 and refused to affirm the “1992 Consensus”³⁹ in the PRC context, tensions across the Taiwan Strait have

³⁶ Elleman, *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy*, p. 131.

³⁷ *Ibid.*, p. 132.

³⁸ Elleman, *High Seas Buffer: The Taiwan Patrol Force, 1950-1979*, p. 127; Elleman, *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy*, p. 132.

³⁹ “The content of the 1992 Consensus is, in fact, quite complex. First, both sides of the Strait have different definitions and interpretations of the term. The ruling Chinese Communist Party evokes the term to indicate that both the Mainland and Taiwan belong to ‘one China,’ and both aim at ultimate unification under the ‘one country, two systems’ framework. Their counterparts in Taiwan take a different view. The Kuomintang (KMT, the ruling party on Taiwan from 1949-2000 and 2008-2016) argues that the Consensus simply indicates that both the Mainland and Taiwan belong to one China; however, the interpretations on ‘China’ are different on both

also increased. The PRC has been squeezing Taiwan's international space by, for instance, convincing three Latin American countries to sever ties with Taipei and recognize Beijing, threatening US companies that depict Taiwan as a distinct geographic entity, and compelling Delta Airlines to publicly apologize for not calling Taiwan a "province of China" on its website.⁴⁰ And as "the PRC has arguably spent the most time and money building a comprehensive military-support infrastructure in the South China Sea that might allow it to one day obtain its strategic goals through force"⁴¹ than all the other countries combined that have an interest in those waters, it seems that a new Cold War is about to arise from strategic competition between the US and PRC.

In this contemporary context of US-PRC strategic competition and a looming Cold War, it seems that Taiwan has once again become strategically important to the US, especially in the US framework of Indo-Pacific strategy. The current US national security advisor John Bolton has suggested in a January 2017 commentary before he took the NSA position that Washington "could enhance its East Asia military posture by increasing US military sales to Taiwan and by again stationing military personnel and assets there. Bolton argues that Taiwan is closer to the

sides. For China, 'one China' refers to 'the People's Republic of China,' but for Taiwan, 'one China' refers to 'the Republic of China.'" Austin Wang, Charles K.S. Wu, Yao-Yuan Yeh, & Fang-Yu Chen, "What Does the 1992 Consensus Mean to Citizens in Taiwan?" *The Diplomat*, November 10, 2018, <https://thediplomat.com/2018/11/what-does-the-1992-consensus-mean-to-citizens-in-taiwan/>

⁴⁰ Vice President Mike Pence's Remarks on the Administration's Policy Towards China, October 4, 2018, Hudson Institute, Washington D.C., USA.

⁴¹ Elleman, *Taiwan Straits: Crisis in Asia and the Role of the U.S. Navy*, p. 143.

Chinese mainland and disputed islands in the South China Sea than either Okinawa or Guam – giving US forces greater flexibility for rapid deployment throughout the region should the need arise.”⁴²



U.S. Vice President Michael Pence said that a Chinese naval vessel came within 45 yards of the USS Decatur in the South China Sea, forcing the ship to quickly maneuver to avoid collision. (Source: White House)

In fact, after the US sent a cruiser and a destroyer through the Taiwan Strait on October 22, 2018, Taiwan’s minister of defense Yen Teh-fa confirmed that US Navy ships had actually already previously sailed through the Taiwan Strait as many as ten times in 2015.⁴³ The

⁴² Gary Sands, “Will Bolton Push for US Troops on Taiwan?” *Asia Times*, April 6, 2018, <http://www.atimes.com/will-bolton-push-us-troops-taiwan/>

⁴³ Hsu Yu-wei, “US Navy ships sailed through the Taiwan Strait 10 times or 10 US Navy ships sailed through the Taiwan Strait? Yen Teh-fa: Their meaning is the same,” *United Daily News*, October 25, 2018, <http://udn.com/news/story/10930/3441793>

significance of the October 22, 2018 transit is that a cruiser, which is a better warship than a destroyer was sent together with a destroyer. In fact, the two destroyers sent together on July 7, 2018, already constituted the ship composition of the regular TPF. Although US Navy ships sailed through the Taiwan Strait as many as ten times in 2015, it was one ship at the time.⁴⁴ On the other hand, the main difference between the 2015/2018 transits and the intermittent Seventh Fleet patrol from 1969 to 1979 is that in 2015/2018 US Navy ships just sailed through the high seas to exercise freedom of navigation without making ports of call.

In terms of the South China Sea, the US defense authorities have sought to coexist with the PRC where possible while also pushing back on what the US sees as the PRC's militarization of the region. According to US military statistics, "the US Navy has had 18 unsafe or unprofessional encounters with Chinese military forces in the Pacific since 2016."⁴⁵ The US Air Force has also had at least one such encounter during the same period.⁴⁶ In February, May and July 2016, at least three of those incidents involved "Chinese fighter jets making what the US considered to be 'unsafe' intercepts of Navy surveillance planes."⁴⁷ The US Navy's most recent encounter with PRC forces occurred on September 30, 2018, while the "destroyer USS Decatur was sailing within 12 miles of two of

⁴⁴ Ibid.

⁴⁵ Ryan Browne, "US Navy has had 18 unsafe or unprofessional encounters with China since 2016," *CNN*, November 3, 2018, <https://edition.cnn.com/2018/11/03/politics/navy-unsafe-encounters-china/index.html>

⁴⁶ Ibid.

⁴⁷ Ibid.

the Spratly Islands as part of what the US calls a ‘freedom of navigation operation’.”⁴⁸ A Chinese destroyer came within 45 yards of the US destroyer, forcing the US destroyer to maneuver to avoid a collision. “The US labeled the Chinese warship’s actions unsafe and unprofessional, while Beijing said the US was threatening the safety and sovereignty of China.”⁴⁹ Commander Nathan Christensen, the US Seventh Fleet spokesman, said after the incident that “U.S. Forces operate in the Indo-Pacific region on a daily basis, including the South China Sea. As we have for decades, our forces will continue to fly, sail and operate anywhere international law allows. All operations are designed in accordance with international law and demonstrate that the United States will fly, sail and operate wherever international law allows. This is true in the South China Sea as in other places around the globe.”⁵⁰

In conclusion, the author of this article recommends that, in the best interest of Taiwan in defending the country’s freedom and democracy, Taiwan’s maritime policies should overlap with the national interest of the US and like-minded countries in exercising freedom of navigation in the Indo-Pacific region. At present, Taiwan has actual control over some of the islands in the South China Sea, such as Tai-ping (Itu Aba), one of the main islands of the Spratly Islands, and Pratas Island. Taiwan should

⁴⁸ Ibid.; Ben Werner, “Destroyer USS Decatur Has Close Encounter with Chinese Warship,” *US Naval Institute News*, October 1, 2018, <https://news.usni.org/2018/10/01/37006>

⁴⁹ Ryan Browne, “US Navy has had 18 unsafe or unprofessional encounters with China since 2016,” *CNN*, November 3, 2018, <https://edition.cnn.com/2018/11/03/politics/navy-unsafe-encounters-china/index.html>

⁵⁰ Ben Werner.

make the seaports of Tai-ping (Itu Aba) or Pratas accessible and be prepared to cooperate with the US and like-minded countries whenever the situation arises, such as a call for humanitarian aid, that Navy ships of the US and like-minded countries need to come aground at the seaports of the islands. Taiwan moreover should make Taiwan's seaports available for US Navy ships to make ports of call again in the same spirit as in 1950-1969 to prevent a possible invasion from the PRC.

∞

Dr. Catherine Kai-ping Lin is a postdoctoral fellow at the Institute for National Defense and Security Research. Her research field is on the interaction of Taiwan's nationalisms with Taiwan's arms procurement from the United States. Dr. Lin holds a PhD degree in Diplomatic History from Georgetown University. She also received a master's degree in international Relations from Yale University and a Bachelor's degree in International Relations from Brown University.

∞

Submission

The journal of *Defense Security Brief* is the official publication of the Institute for National Defense and Security Research (INDSR). Articles express the authors' views only and are not necessarily the official policy of INDSR or the editors of the journal.

Defense Security Brief accepts original articles, review, comments and case studies. Contemporary international affairs, defense, security, Indo-Pacific issues and policy reviews are welcomed. The editorial review process can take up to three months. The editorial reserves the right to accept, reject or alter all editorial and advertising material submitted for publication. Manuscripts should address to min.chou@indsr.org.tw, in Microsoft Word format. Hard copies will not be accepted by *Defense Security Brief*.

To submit an article, authors are advised to follow these guidelines:

- Manuscript are around 1500-4500 words long including footnotes.
- Any tables or charts should be supplied in separate files, ideally not linked to text around it.
- Footnote references should be complete and include first and last names of authors, titles of articles (even from newspapers), place of publication, publisher, exact publication dates, volume and issue number (if from a journal) and page numbers. Web sources should include complete URLs and DOIs if available.
- A short author's biography of four or five lines should also be included. This information will appear at the last page of the article.

Note: *Defense Security Brief* are available for download from INDSR's website, indsr.org.tw.

