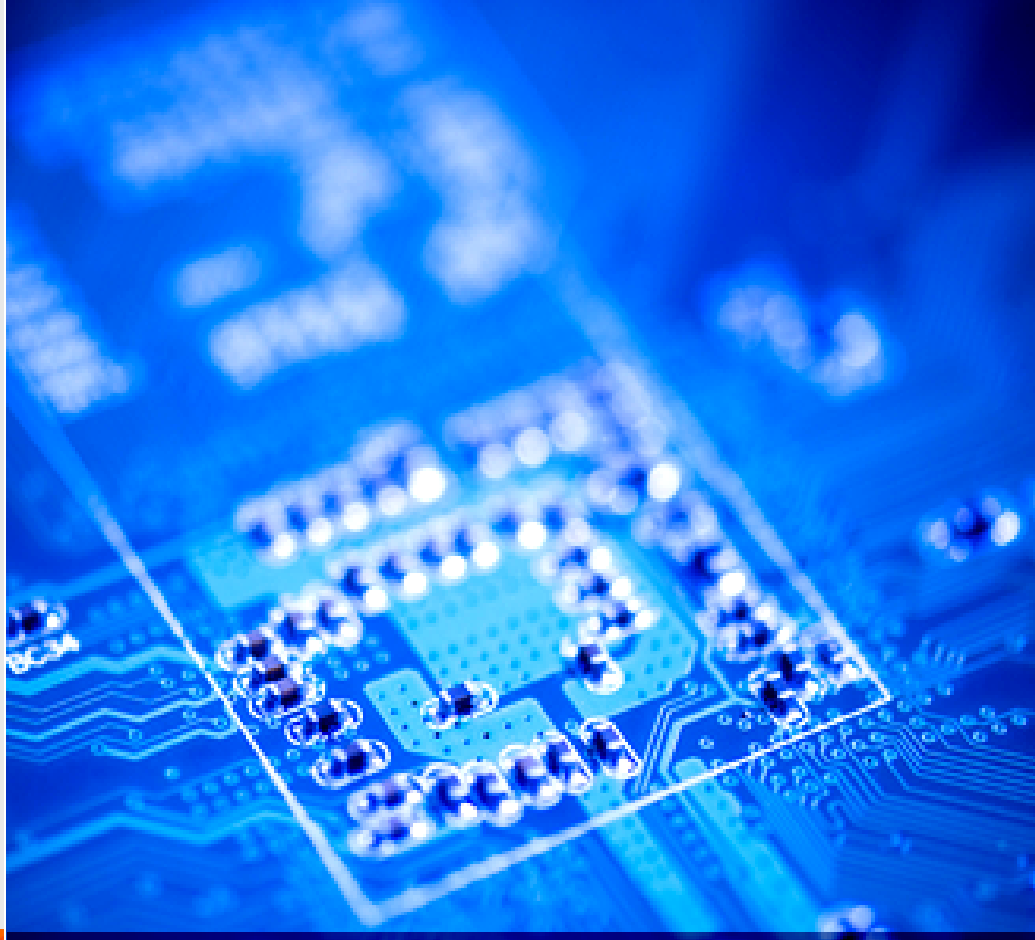


Revolutionizing Taiwan's Security

Leveraging C4ISR for traditional and non-traditional challenges

Mark A. Stokes

PROJECT 2049 INSTITUTE

About the Project 2049 Institute

The Project 2049 Institute seeks to guide decision makers toward a more secure Asia by the century's mid-point. The organization fills a gap in the public policy realm through forward-looking, region-specific research on alternative security and policy solutions. Its interdisciplinary approach draws on rigorous analysis of socioeconomic, governance, military, environmental, technological and political trends, and input from key players in the region, with an eye toward educating the public and informing policy debate.

www.project2049.net

An example of a surveillance radar system that enhances air sovereignty and situational awareness.

Source: 2009 National Defense Report, Ministry of National Defense, R.O.C.

Cover illustration: an integrated circuit chip similar to those found in almost all civilian and military electronics.

Source: Exponent.

Contents:

Abbreviations 3

Executive Summary 5

Introduction 7

A Review of the Threats 9

Taiwan's Response: an All-Hazards Transformation 17

Conclusion 34

References 36

Abbreviations

ASW	Anti-submarine warfare
CNO	Computer Network Operations
COTS	Commercial off-the-shelf
CSIST	Chungshan Institute of Science and Technology
ECM	Electronic Countermeasures
EMP	Electromagnetic Pulse
FPGA	Field Programmable Gate Array
GEOSS	Global Earth Observation System of Systems
HEMP	High-Altitude Electromagnetic Pulse
HF	High Frequency
H5NI	Avian/Bird Flu, a subtype of Influenza A virus.
ICT	Information and communications technology
IMSE	Improved Mobile Subscriber Equipment
IP	Internet Protocol
IRST	Infra-red Search and Track
JTIDS	U.S. Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
Kbps	Kilobytes per second
MANET	Mobile Ad Hoc Networks
Mbps	Megabytes per second
MDA	Maritime Domain Awareness
MESA	Mobile Enhanced Situational Awareness
MICS	Military Information and Communication System
MND	Ministry of National Defense (Taiwan)
NASA	National Aeronautics and Space Administration
NHCC	National Health Command Center
NOAA	U.S. National Oceanic and Atmospheric Administration
OTH	Over-the-Horizon
PCL	Passive Coherent Location
PCS	Process Control Systems
PLA	People's Liberation Army

PRC	People's Republic of China
ROC	Republic of China
SAR	Synthetic Aperture Radar
SDR	Software-Defined Radio
TIEOS	Integrated Earth Observation System
UMPC	Ultra-Mobile Personal Computer
UWB	Ultra-wideband
VHF	Very High Frequency
WiMAX	Worldwide Interoperability for Microwave Access

Executive Summary

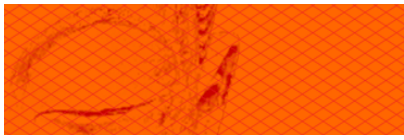
No capability is more important than command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). C4ISR systems reduce surprise, increase warning time of emergencies, facilitate the sharing of information within an emergency response network, and allow senior decision makers to make better-informed decisions. Although hardware is important in times of emergency, weapon systems are of limited utility without an advanced C4ISR system in support.

At the heart of C4ISR is information technology, an area in which the Republic of China (Taiwan) has long enjoyed an international competitive advantage. It is one of the world's most innovative societies, given its status as a hidden yet critical node in the global information technology supply chain and the holder of one of the world's largest number of utility patents. Paradoxically, while the island's private sector is a world leader, the ROC's defense and homeland security establishments have lagged behind in leveraging the information revolution.

However, Taiwan's information technology paradox is changing. The ROC has the potential to harness its innovative strengths in information technologies in order to meet some of the world's most stressing security challenges. The People's Republic of China (PRC) and its ruling Chinese Communist Party present a daunting and growing military threat that is rivaled only by the dizzying array of non-traditional security hazards that often go unheeded. Taiwan's society is one of the world's most vulnerable to natural disasters, and is also challenged by the prospect of pandemics, control of its borders, and terrorism and forms of extremism.

Given this severe set of security challenges, Taiwan has powerful incentives to field one of the most advanced and networked emergency management C4ISR systems in the world. Whether military or civilian, responses to all hazards require maximal situational awareness and the means to react efficiently and effectively to prevent a further deterioration of the situation. Perhaps best exemplifying Taiwan's position at the cusp of the information revolution is the recent introduction of one of the world's most sophisticated advanced tactical data link networks. The number of participants in the network today remains limited. However, assuming proper training and cultural adjustments can be managed, the gradual expansion of the advanced data link network will solidify Taiwan's position at the leading edge of the network-centric information revolution.

However, there is more that could be done to leverage C4ISR for all-hazards defense. Enhancements to its command and control system, especially in the area of anti-submarine warfare (ASW) and maritime domain awareness, would better prepare the island's civil and military leadership for emergency situations. Other investments could be worth considering such as advanced voice communication technologies and dual-use space systems (including electro-optical and synthetic aperture radar (SAR) remote sensing and broadband communication satellites) could prove invaluable to disaster warning, recovery, and response. These capabilities also may satisfy verification requirements in any future cross-Strait arms control regime.



Finally, Taiwan's security challenges are unique and more severe than most. As a result, Taiwan's successes in innovative approaches to mitigating hazards may be instructive for defense and homeland security establishments around the world.

Introduction

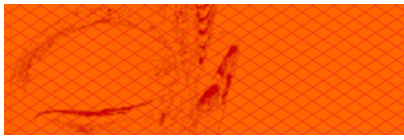
The global information revolution is a phenomenon that is transforming the world's industrial-based societies and economies. In our everyday lives, we look to information and communications technology to work, function, cooperate, and compete more effectively. Countries have also harnessed the information revolution to bolster their national security and defense establishments. The trend towards increased computing power to process, collate, and analyze a vast quantity of sensor data in order to mitigate and respond to a range of security challenges has turned the information revolution into the C4ISR revolution.

Leading the information revolution is the ROC, a hidden yet critical node in the global technology supply chain.[1] Despite its central role, Taiwan is lagging behind most advanced societies in effectively leveraging the information revolution for its own defense and non-traditional security challenges. However, this has been changing. Tested by some of the world's most stressing security challenges, Taiwan's political and military leadership increasingly understands the value of resilient sensor networks, communications systems, and command and control networks in mitigating and responding to large-scale crises.

Success or failure in responding to emergencies depends upon the quality of information available to decision makers and the manner in which it is used. Analogously, individual decisions and actions depend upon the information about the environment and potential dangers perceived by sensory system. The brain acts as a centralized decision making center that automatically processes millions of bits of information to formulate the optimal response. Once a course of action is determined, signals are transmitted to the relevant response mechanisms. However, if there are faults in the cognitive or central nervous system in an emergency situation, it may be difficult to mount even the most basic of defenses such as calling for help. No matter how physically strong an individual may be, a failure at any point in this sequence can be fatal to his or her threat response.

The same principle applies toward a country's security "sensory system." Here lies the critical function of a command, control, communications, computers, intelligence, surveillance, and reconnaissance, or C4ISR system, in supplying critical data to the decision making center in the government and then relaying coordinated responses to both military and civilian peripheries in the network. Shortcomings in disaster management throughout history can often be traced back to a C4ISR-related weakness. Therefore, to prepare for and defend against the full range of man-made and natural security hazards, many countries have made significant investments in the realm of C4ISR.

Taiwan has powerful incentives to leverage the global information revolution in order to field one of the world's most advanced C4ISR systems. Highly prone to natural disasters and facing a sizable challenge from the Chinese People's Liberation Army (PLA) across the Taiwan Strait, it is perhaps the most dangerous location on earth. Further complicating its ability to prepare for national emergencies is Taiwan's political isolation within the international community. However, advances in information technology could revolutionize national emergencies management in a way that offsets Taiwan's isolation, and facilitates linkages with the United States as well as the rest of the international community before and during crisis situations.



As a case study, Taiwan's experiences in leveraging C4ISR for all-hazards defense should be of interest to U.S. policy makers, warfighters, Congress, and emergency management authorities. Due to the severity of its threat environment, Taiwan's success and failures may offer lessons to inform our own homeland security. While much collaboration has been done to date, the United States is expected to continue to play a critical role in assisting Taiwan in its self-defense, as outlined in the Taiwan Relations Act (TRA).

This monograph outlines the security challenges that Taiwan faces and how it is leveraging C4ISR to meet those challenges. The first section addresses the military challenge that the People's Republic of China (PRC) poses to Taiwan's C4ISR system, as well as other hazards to Taiwan's security, such as natural disasters, pandemics, and terrorism/extremism. Based on these challenges, the second section addresses fundamental situational awareness requirements and discusses communications, and command and control issues. The final section summarizes how Taiwan is meeting these challenges and offers preliminary suggestions for consideration.

A Review of the Threats

Taiwan faces a unique and severe set of man-made and natural challenges to its national security. Man-made threats include the conventional use of military force and other forms of organized violence, such as terrorism. Natural hazards include disasters and pandemics. This section outlines the most severe threats to national security that could result in high loss of life, political instability and economic setbacks. Addressing these hazards will require thorough planning, as crises are often multitudinous. For example, mudslides can follow a major typhoon, or a public health crisis can follow a military confrontation.

The PRC Military Challenge to Taiwan's C4ISR Infrastructure

The potential for the PRC to use military force to resolve its political differences with Taiwan is the most dangerous and stressful of the possible hazards. This scenario will undoubtedly test Taiwan's ability to coordinate military responses and manage the civilian emergency management system; all of which will depend upon sustaining situational awareness as well as effective communication both within and beyond the island. At the heart of this management and coordination lies the national and operational level command and control system. Because of its critical function, the system is likely to become target of attacks.

A central element of the PRC's strategy would be to exploit, deny, or manipulate communications transmitted via Taiwan's civil and defense information infrastructure, and electromagnetic environment. As one basic PLA primer on campaign theory asserts, "seizing information dominance, and denying the enemy of his information capabilities, has become the most important task of modern theater operations."[2]

Under extreme conditions of information dominance, Taiwan's political and military risk calculations, as well as its ability to effectively coordinate a response, would be significantly affected.[3] Furthermore, even if operational capability is retained at the tactical level, the loss of situational awareness within a centralized command and control structure and the ability to communicate with fielded forces has the potential to accelerate a rapid collapse of defenses.

Electronic Countermeasures: Back to the Basics

A key feature of a PLA information operations campaign would be electronic warfare, which seeks to complicate an adversary's maneuvers in an increasingly complex electromagnetic environment. PLA advances in this area should provide an impetus for Taiwanese policymakers to prioritize preparations for this contingency.[4] The PLA's senior leadership understands that control over the electromagnetic spectrum can be a crucial determinant of a conflict. Since the United States' successful attacks on Iraqi communication networks in the 1991 Gulf War, the PRC's senior military leadership has stressed the strategic importance of electronic warfare as a component of information warfare. In 1995, Admiral Liu Huaqing, Vice Chairman of the Central Military Commission asserted:

> *"Information warfare and electronic warfare are of key importance, while fighting on the ground can only serve to exploit the victory. Hence, China is more convinced (than ever) that as far as the PLA is concerned, a military revolution with information warfare as the core has reached the stage where efforts must be made to catch up with and overtake rivals."*[5]

The importance that the PLA places on targeting the opponent's electromagnetic spectrum reflects a solid understanding of information and electronic warfare in defense planning. In particular, PLA operational concepts emphasize the importance of centralized command and control over their electronic attack assets and the role of electronic warfare in successful deception and surprise against their opponent.

Scenario: A PLA Electronic and Information Attack Against Taiwan

A PLA electronic warfare campaign could pose challenges to the integrity and reliability of Taiwan's situational awareness and communications by disrupting wireless, satellite, and radar networks. The basic objectives of an electronic attack campaign would be to complicate Taiwan's ability to detect enemy preparations and subsequently mount an effective defense against possible air and missile strikes. Airborne, maritime, and land-based jammers would disrupt early warning and air defense radar systems, especially those supporting missile defenses. Decoys would be used to force Taiwan's air defense system to cover a 360-degree area while deception jamming would create false aircraft returns and trigger activation of radars. In short, electronic warfare operations would be integrated with the physical destruction of command and control centers, early warning sites, and air defense systems to reduce the effectiveness of an enemy's communications system and to effect systemic paralysis.[6]

The PLA places a high priority on disrupting communications networks. In conjunction with strikes, PLA planners indicate that electronic countermeasures (ECM) assets would target leadership and operational-level communications. Airborne communications jamming packages would interrupt early warning broadcasts and leadership communication networks, as well as ground-to-air and air-to-air communications. Broadband jamming could deny Taiwan's armed forces a significant portion of the frequency spectrum. Carrying the inherent risk of undermining its own communications, PLA writings indicate significant investment into overcoming this challenge.[7] PRC technical writings also indicate an interest in developing the means to disrupt advanced tactical data link networks, such as the U.S. Joint Tactical Information Distribution System (JTIDS).[8] In addition, false communications networks would be launched to imitate real ones in an attempt to deceive Taiwan and U.S. intelligence assets.[9]

Electronic warfare likely would be conducted along with other forms of information operations. PLA computer network attack specialists discuss targeting automated enemy command systems through saboteurs who have penetrated internal networks and/or through pre-planted viruses into automated air defense networks.[10] Authors also discuss 'intelligence warfare,' which is "the use of every type of sensor and other capabilities to attain the necessary level of intelligence while destroying or degrading the enemy of his sensors in order to deny him his needed sources of intelligence."[11] Together, electronic and intelligence

warfare could deny Taiwan's national and military leadership critical access to the electromagnetic spectrum.

Non-Conventional Electromagnetic Attack. The PRC's research and development community has been investing resources in more exotic forms of electronic warfare. In particular, efforts have been directed toward an energy weapon that produces a strong electromagnetic pulse (EMP) to neutralize electronic systems within its effective radius. Known as a high-powered microwave [HPM; 高功率微波武器] device, it has been championed by many of China's most respected advocates of information warfare. PLA-affiliated research institutes have already mastered certain power sources commonly associated with microwave weapons.[12] Chinese writings indicate various applications for HPM devices to shut down adversarial radars and C4ISR systems in an opening salvo, including directional systems for jamming the electronic systems of attacking aircraft, anti-radiation missiles, and as an anti-satellite weapon to degrade sensitive satellite electronic systems.[13]

The size of a HPM device depends upon the target, delivery application, and desired effects. For the PRC, the obstacle lies in weaponizing a HPM device that could release the required amount of energy at the calculated range and on target. However, if the PRC is able to overcome these challenges, an operational HPM warhead could be sized to fit a space similar to that available in the nose section of a conventional short range ballistic or land attack cruise missile.

Terrorists are also believed to be increasingly capable of fielding a crude HPM capability. Smaller HPM weapons are becoming increasingly well-suited for terrorists and saboteurs, including "hand-held" missions that could employ a system that weighs less than ten pounds. Strategic facilities, such as Taiwan's science parks, could serve as ideal targets for terrorists or saboteurs. Around the world, several high-power microwave technologies, using commercial off-the-shelf (COTS) technology, are now readily available for use in operational weapons. For example, existing EMP generators already have the ability to upset or destroy present generation digital electronics.[14]

Another potential challenge is the detonation of a nuclear device in the upper atmosphere to generate a high-altitude EMP (HEMP) burst to disrupt electronic systems. Once detonated, HEMP changes the ionization of the ionosphere and magnetosphere, which will affect critical communication links, radar transmissions, and electro-optic sensors.[15] The 2005 report to Congress on *Military Power of the People's Republic of China* highlighted the possibility of that the PRC could use such a capability as part of a larger campaign to "intimidate, if not decapitate, the Taiwan leadership."[16]

A HEMP or HPM attack could have a ripple effect on the electronic fabric the supports Taiwanese society. If used against a critical node, a device likely would have a significant effect on Taiwan's national information infrastructure, public switched telephone network (PSTN), and international links due to its reliance on electronic information systems. Strikes against foundations in Taiwan's critical infrastructure and strategic industries, such as Hsinchu Science Park, could have systemic or even global consequences.[17]

Computer Network Attack. Electronic warfare is also becoming integrated with computer network operations (CNO) that target the opponent's network information systems that could be strategically exploited to the PLA's advantage. An attack campaign would likely target

automation systems, such as process control systems (PCS), which are extensively used in managing electric power, water, petroleum, natural gas, as well as communications systems. If a PCS could be undermined, there may be no need for the network's physical destruction. Similarly, he attacks would also be aimed at supervisory control and data acquisition (SCADA) systems that are also critical to the secure and efficient operations of critical infrastructure.[18]

The computer network attacks in Estonia in 2007 are illustrative of the dangers faced by Taiwan. For three weeks, many of the government, banking, and media sites and computer systems were subjected to a massive denial-of-service attack (when a target site is bombarded with so many false requests for information that it crashes).[19] Estonia's experience and the daily occurrence of similar attacks throughout cyberspace demonstrate that waging a cyber war is not beyond the capacity of any technologically capable nation.

To defend government and private sector computer networks, Taiwan's national-level authorities created a Computer Emergency Response Team, while the Ministry of National Defense (MND) established an Information and Electronic Warfare Command. Although Taiwan has taken necessary precautions against CNO threats, intrusions upon sophisticated networks in the U.S. testify that this new cyber frontier cannot be completely safeguarded.[20]

Coordinating information and electronic campaigns

In a conflict scenario, joint electronic countermeasures operations would be coordinated within the Joint Campaign Command's Joint Electronic Countermeasures (ECM) Center (*lianhe dianzi duikang zhongxin*; 联合电子对抗中心). The Center's responsibilities include: directing the collection and analysis of electronic reconnaissance; developing the ECM concept of operations (*juexin*) and electronic attack plan; assigning responsibilities and targets, transmitting orders to service ECM organizations; and coordinating with the Joint Theater Command leadership and other centers.[21]

PLA sources indicate that a typical ECM regiment includes a headquarters department, a political department, a logistics department, and a technology department. The regiment would include an electronic reconnaissance battalion, a communications jamming battalion, a radar jamming battalion, and a radar camouflage battalion. The reconnaissance battalion [侦察战] oversees both fixed sites and mobile units for collection, analysis, and exploitation of communications and radar intelligence. The land-based information collection is augmented by airborne and maritime assets.[22]

The Nanjing Military Region's ECM Regiment [the 73676 Unit] is the electronic warfare unit most likely to be engaged in a Taiwan scenario. Located in the Binhu district of Wuxi [无锡], the regiment has at least four battalions. One source indicates that the 2nd battalion of the Wuxi ECM unit is equipped with new high-powered jammers [大功率干扰]. There are also suggestions that an additional battalion or group is located in the Tong'an [同安] area of Xiamen. Some group armies, such as the 31st near Xiamen, have an ECM battalion [营] or group [大队].[23] PLA army aviation units are said to have specialized heliborne ECM assets for jamming both communications networks and radar systems.[24] In addition, PLA electronic warfare units are equipped with ultra high frequency (UHF) satellite communications jamming assets.[25]

Natural Disasters

The PLA is not the only security challenge that Taiwan faces. In the wake of a major typhoon that struck Taiwan in August 2009, ROC President Ma Ying-jeou proclaimed "our enemy is not necessarily the people across the Taiwan Strait, but nature." In recognizing that natural disasters pose as much if not more of a danger than PRC military action, he also warned "as a result of climate change, disasters like Morakot are not that unusual now, so we have to be prepared for the worst."[26]

Natural disasters indeed pose a salient threat to Taiwan. In 2005, the World Bank assessed that "Taiwan may be the place on Earth most vulnerable to natural hazards, with 73 percent of its land and population exposed to three or more hazards."[27] Typhoons, floods, landslides, earthquakes, and other disasters can result in significant human and economic losses – both in terms of tangible economic costs and diminishing GDP. Similar to the scenario of a military attack, such events also pose significant challenges for Taiwan's early warning, communications, and emergency response management. Enhancing these capabilities could mitigate the losses associated with natural disasters, an investment that would prove valuable as Taiwan is expected to experience a higher volume of natural disasters in the future.

Typhoons. Typhoons make up at least 70% of Taiwan's natural disasters and the country often suffers significant human casualties and economic loss from the violent winds and extreme rainfall. According to one estimate, typhoons result in an annual economic loss of around NT $20 billion.[28] The deadliest typhoon in recorded history, the 2009 Typhoon Morakot, left a toll of over 500 victims and estimated financial losses of U.S. $3.4 billion (NT $110 billion). Morakot also caused significant damage to the island's communications, including loss of 1700 wireless base stations and six undersea cables carrying international traffic.[29]

The incidence of typhoons in Taiwan has risen from an average of 3.3 times per year in the 20th century to an average of 5.7 times per year after 2000.[30] The increased frequency, as well as intensity, of typhoons has been associated with warming sea temperatures. Therefore, as the island's senior political leadership has noted, the typhoon prognosis for Taiwan is bleak, with climate change projected to further increase ocean temperatures.[31]

The aftermath of Typhoon Morakot (left to right): Military troops evacuate survivor; homes collapsed due to flooding and the military removing debris from the typhoon.

Source: AFP/Getty images and AP

Floods and Landslides. Typhoons are linked with floods and landslides. Taiwan's unique geography features 156 mountain peaks surpassing 3,000-meters (10,000 feet) that create one of the sharpest drops in elevation in the world. Coupled with annual rainfall totaling 2.5 times the world's average, Taiwan's steep slopes have created volatile rivers with the largest discharge per unit drainage area and shortest time of concentrations in comparison to others around the world.[32] The intense rain and rapid water flow result in erosion, which is compounded by frequent earthquakes that undermine the stability of mountains and hillsides.[33]

Earthquakes. Exacerbating the flood/landslide problem are earthquakes. Located at the world's most seismically active geological intersections, Taiwan is a collision zone between the Philippine Sea and Eurasian tectonic plates. More than 200 earthquakes can be felt on the island every year, and the frequent earthquakes have had devastating consequences. More than 3000 perished in a 1935 earthquake, and the Chi-Chi earthquake in 1999 claimed 2500 lives. In addition to damaging critical information infrastructure, Taiwan's annual economic loss from earthquakes since 1900 is estimated to be 0.7% of its GDP.[34]

Tsunamis. Often forgotten are tsunamis, which are low-probability disasters with very large impacts that are can be caused by underwater earthquakes. Localities in the Asia-Pacific region experience damage from a tsunami every year or two, and region-wide events occur a few times each century. The 2004 Indian Ocean tsunami serves as a stark reminder.[35] Before the 2004 tsunami, Taiwan was often cited as suffering the greatest losses from a tsunami in 1782. In modeling and simulation studies, engineers believe that the two potential sources could be the Manila Trench, which runs north to south in the Bashi Strait and off the coast of Luzon, and the Ryukyu Trench, which runs up from Hualian and the Ryuku Islands. In one scenario, southern Taiwan could be hit with a wave 11-meters in height, with flooding reaching 8.5-kilometers inland.[36] The key to mitigating the effects of a tsunami would be early warning and assured communications. Representatives from Taiwan's scientific community have called for a system capable of providing early warning of off-shore seismic and other events, perhaps linked to the Pacific Tsunami Warning Center.[37]

Pandemics

As noted, threats from the PLA and natural disasters can have severe consequences for Taiwan if they occur in the absence of an effective early warning network, resilient communications, and an efficient disaster management system. However, in terms of the human toll, pandemics may be even more catastrophic. Scientists believe that a major influenza pandemic, emerging from birds and pigs, is almost unavoidable, and is most likely to originate from China or Southeast Asia.[38]

Taiwan's proximity to the epicenter, its integral role in regional trade with China and Southeast Asia, and widespread urbanization and high population density exponentially heightens its exposure to potential pandemics. It is also a waypoint in Asia for migrant birds, which have been suspected as a source for the deadly H5N1 virus (avian flu).[39] Between 42,000 and 62,000 people died in Taiwan during the influenza pandemic of 1918-1920. One study found that an influenza outbreak, similar in scale to that of 1918, could cause up to 315,000 casualties.[40]

A pandemic will have the potential to disrupt all facets of a functional society. According to one comprehensive report, high employee absenteeism rates are expected, which could disrupt businesses and essential services such as hospitals, police, fire, utilities (water, electricity, and communications), garbage pickup, and food distribution. While it may not cause physical damage, a pandemic could threaten critical infrastructure by affecting essential personnel for extended periods of time.[41] A vaccine is unlikely to be available in the first four to six months of a global epidemic, since it can only be developed after the newly mutated virus has been identified. A moderate or severe pandemic will severely stress the health care system's ability to provide care for those who need it.[42]

Despite Taiwan's risk factors and potential devastation from a pandemic, it is absent from risk indexes and information-sharing mechanisms because it does not hold formal membership in international health organizations. This provides the impetus for Taiwan to strengthen its own defenses against potential pandemics. Preparing and responding to an epidemic have much in common with military planning and operations. A pandemic can be contained through a rapid response that includes surveillance, identification, and isolation of infection as well as a thorough tracing of contacts. Also critical is early warning of a pandemic and the ability to track its spread to commence containment measures. This will also depend upon maintaining accessible channels of communications with the public and among government agencies as well as other public health institutions.

Terrorism, Trafficking, and Border Control

Beyond natural disasters and pandemics, Taiwan also faces hazards associated with proliferation of weapons of mass destruction (WMD), terrorism and trafficking. Taiwan is often viewed as being immune to terrorism, perhaps due to the island's isolation within the international community. Yet, the unexpected is not improbable. A terrorist organization seeking to undermine the global information and technology supply chain could see Taiwan as a target of great economic impact.[43] Furthermore, Taiwan's growing interdependence with the mainland, and, by extension, the PRC's interdependence with the United States, especially in international finance, could draw the attention of China-based terrorists seeking to affect their own government's economic interests close to home.[44]

Weapons of mass destruction. The island's ports have been viewed as a potential transshipment point for weapons of mass destruction. Taiwanese officials have expressed concern for potential terrorist activities, cautioning that a potential hijack or attack on oil carriers or ships carrying dangerous materials would damage Taiwan's harbors and key coastal infrastructure. This in turn will negatively impact on Taiwan's economy and interrupt international trade. In recognition of this hazard, Taiwan has been an active participant in U.S.-led global counter-proliferation initiatives, such as the Megaports Program and the Container Security Initiative.[45]

Border Control and trafficking. Despite its maritime geography, Taiwan faces a border control problem. Its coastal areas, coastlines, airports, and other points of entry require constant vigilance against illegal drugs and immigrants, diseases, terrorists, and weapons of mass destruction. The movement of people has presented a security challenge since the end of martial law in 1987. Human smuggling allegedly peaked from 1990 to 1993, during which 5,000 PRC nationals illegally entered Taiwan each year. While the numbers have declined,

authorities still recorded 2,500 aliens illegally entering Taiwan in 2005. Observers have noted that the number of illegal immigrants could be three to five times higher than official numbers reflect. Most enter Taiwan as part of a human trafficking network for prostitution. The challenge of managing migration across national borders could be exacerbated by an influx of arrivals in the event of significant internal turmoil in China.[46]

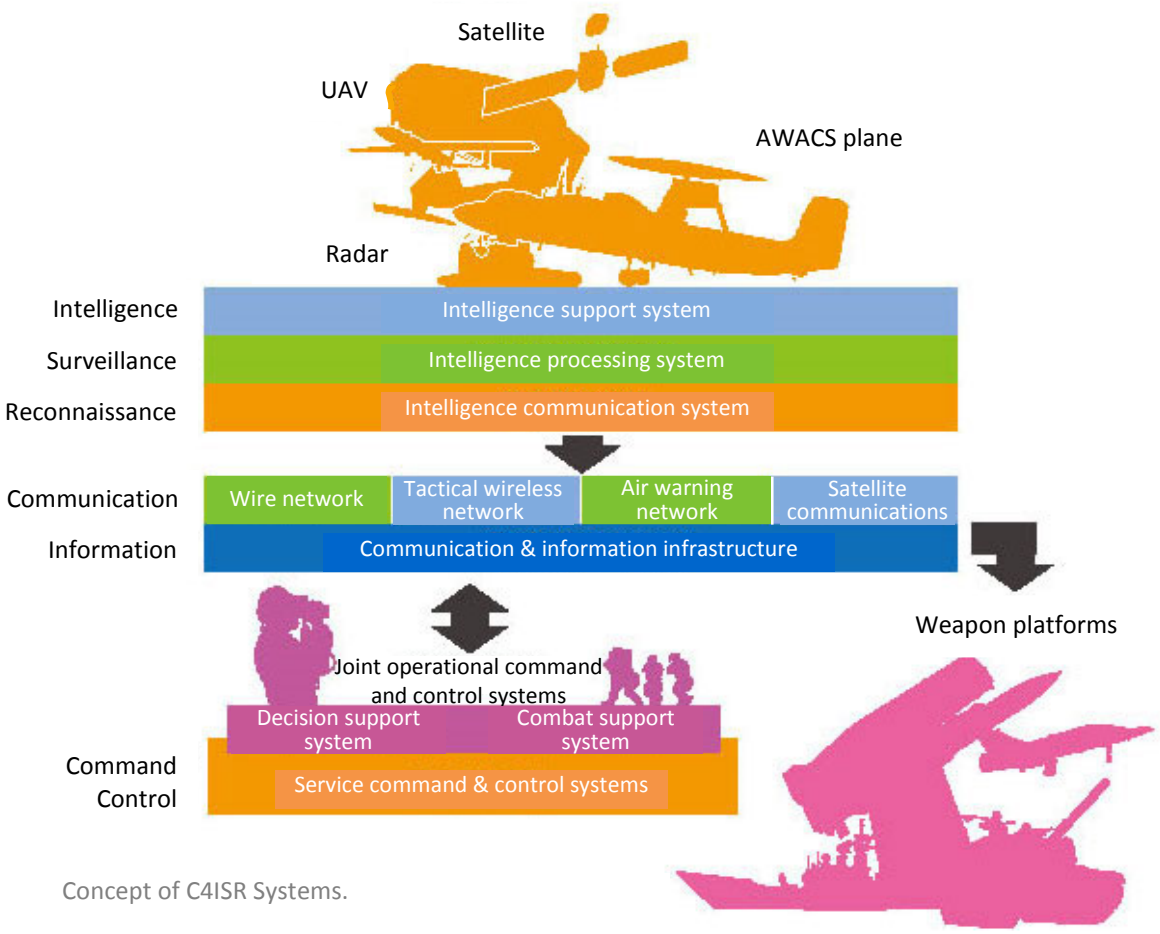
Taiwan's Response: an All-Hazards Transformation

All of the security challenges threats discussed above share commonalities that could benefit from an integrated all-hazards approach to threat mitigation. An integrated all-hazards approach to emergency management ties together central government resources to prevent, prepare for, respond to, and recover from military use of force, major natural disasters, terrorism, and other emergencies. The desired end result is improved coordination among central, city, and county organizations, which helps to save lives and protect communities. An all-hazards C4ISR system could enhance the effectiveness and efficiency of the national command and control system under stressful conditions. Although individual threat scenarios require tailored responses and mission-specific C4ISR systems, all-hazards planning and programming would seek universal, interoperable capabilities that could feasibly apply to a full spectrum of emergencies where possible.

Prioritizing C4ISR

Over the last decade, Taiwan has made significant advances in its defense and emergency preparedness through C4ISR modernization. Driven in part by the desire to establish Taiwan as a logistics and communications hub in the Asia-Pacific region, initial moves to accelerate the development of an advanced national information infrastructure began in 1994. In a separate but related effort, Taiwan's Ministry of National Defense (MND) made its first formal request to the United States for an advanced tactical data link system and four E-2 airborne early warning (AEW) aircraft in 1992. While the E-2 AEW request was approved, U.S. policymakers deferred a decision on advanced tactical data links as it was considered to have surpassed Taiwan legitimate defense requirements at the time. Taiwan's MND resubmitted its request for advanced tactical data links in 1998, and it was subsequently approved in 1999.[47]

The apparent fragility of Taiwan's C4ISR systems and acceleration of PLA force modernization coalesced to bring C4ISR to the forefront in U.S-Taiwan defense relations in the late 1990s. Among the events that focused attention on C4ISR included the July 1999 power outage, the most severe in Taiwan's history, which affected telecommunications throughout northern Taiwan. Followed closely by the Chi-Chi earthquake in September 21, 1999, both incidents resulted in catastrophic failures of Taiwan's telecommunications infrastructure. Acting on a request from Taiwan's MND, DoD conducted a strategic level assessment of Taiwan's national command and control system and C4ISR vulnerabilities. A subsequent MND-sponsored MITRE assessment conducted in 2002 surveyed Taiwan's national, operational, and tactical level C4ISR requirements. The MITRE study is said to have outlined a comprehensive C4ISR blueprint to help guide Taiwan's unique requirements. Having merged the broader C4ISR initiative with advanced tactical data links, senior Pentagon authorities publicly pronounced in 2003 that C4ISR, centered on the "Po Sheng" ("Broad Victory" or 勝專案) program, was a foremost priority in U.S.-Taiwan defense relations.[48]



Concept of C4ISR Systems.

Source: 2009 National Defense Report, MND, ROC

"Po Sheng" and Taiwan C4ISR Modernization

Since 2001, Taiwan's defense-related C4ISR modernization has centered upon the centrally managed Po Sheng program. Based on MITRE's recommendations, a key goal was to design, develop, and field a common tactical picture (CTP) and common operational picture (COP).

The backbone of the CTP was to be advanced tactical data links, similar to the United States' JTIDS. The theoretical foundation of tactical data links is rooted in German Field Marshall Erwin Rommel's North Africa campaign. One of the keys to his victory was the flexible system of tactical communications that connected individual tanks. The arrangement not only permitted Rommel and subordinate commanders to have greater situational awareness, but also gave junior officers more latitude for independent and decentralized action.[49]

This basic concept has since morphed into what is known today as network centric operations. Network-centric warfare equips soldiers, airmen, and sailors with a COP that significantly increases situational awareness. As a result, individuals and units equipped to participate in the network are able to synchronize action, without necessarily having to wait for orders, which in turn reduces their reaction time. In addition, the network allows for dispersed and

flexible operations at lower cost. Therefore, the introduction of a networked CTP based on advanced tactical data link program is a paradigm shift that could gradually break down Taiwan's traditionally stovepiped, service-oriented approach to defense. As Taiwan expands the number of participants in the network, it could exponentially increase its ability to defend against potential PRC use of force.[50]

Advanced tactical data links, such as those associated with JTIDS, are a key element of network centric operations. JTIDS is a tactical communication system that allows an almost unlimited number of users in a network to share information. The system has the ability to provide precision location or position data that will be critical for tracking or monitoring developments.

In addition to its advanced technological capabilities, JTIDS is also relatively resistant to electronic warfare attacks. Firstly, it operates on a secure and jam-resistant wireless data link network operating in the UHF or L-band portion of the frequency spectrum - specifically between 962 to 1213-MHz. Within this 250-MHz bandwidth range, the JTIDS signal hops at a very high rate (77,000 hops a second) over 51 specific frequencies.[51] As a result, the time spent on any frequency is so short that it is extremely difficult for an adversary to detect and interfere with the signal. Although JTIDS can still be jammed, the cost and power required for a jammer to cover the entire 250-MHz bandwidth would be significant. Secondly, in addition to its frequency-hopping technology, JTIDS also utilizes encryption for an extra level of security.[52]

An example of Link 16 terminal

Source:ViaSat

Lastly, the absence of critical nodes or single points of failure in the network adds resilience to the JTIDS network. Its horizontal structure reduces its vulnerability to attack as there is no central network control authority, each participant in the network is assigned a specific time slot within which to transmit and receive information.

The original Po Sheng concept, valued at more than U.S. $3.5 billion, was ambitious. It envisioned the installation of more than 750 data link terminals on most major weapons platforms that are integrated with joint MND, army, air force, and naval operations centers.[53] The COP and common operating environment components sought to develop and install software and displays into a Taiwan command and control system (TCCS), which would also include the CTP. Other facets included upgrades to Taiwan's fiber optical backbone network, a mobile tactical intranet, and new tactical radio systems for the ROC Army, Navy, and Air Force. The program also envisioned a broadband communications satellite for beyond line-of-sight communications.[54] It is important to note, however, that the Po Sheng program has not included intelligence, surveillance, and reconnaissance capabilities (e.g., unmanned aerial vehicles, radar systems, signals intelligence systems, and space-based sensors).[55]

Due to resource limitations, Taiwan's defense authorities reduced the initial scope of the program by approximately one-third, with plans to expand over the next five years.[56] While representing a significant advance in capabilities, Taiwan's fielded military forces may not realize the full potential of having networked platforms. Nevertheless, even with the limited number of participants in the network, one U.S. defense source familiar with Taiwan's system remarked that "Taiwan has the best common tactical picture in the world today, outside of the United States."[57]

At the same time, the resource constraints caused some to lament a diminished prioritization of C4ISR both in the bilateral dialogue and within Taiwan's MND. Former Deputy Director of the Defense Security Cooperation Agency (DSCA) Ed Ross asserted that:

> *Taiwan's Po Sheng C4ISR program became an ongoing "approved program" with only marginal oversight and direction from DoD policy offices. While everyone involved in program execution on both the US and Taiwan sides have made Po Sheng a successful program, I do not believe it has achieved what it otherwise would have achieved with high-level US policy oversight and support.*[58]

However, recent trends toward an Internet Protocol (IP) data link present new opportunities for C4ISR development. IP data links greatly exceed the speed of JTIDS (2 Mb/sec compared to Link 16's 238 kb/sec), could operate at a longer range (up to 100 miles), and are compatible with a wide array of internet-ready systems.[59] The increased availability COTS information and communications technology (ICT), with only the most sensitive, core functions met with military-specific technologies, raises the attractiveness of this approach. These can also be adopted on a national scale as communications move towards an IP standard, specifically IP version 6 (IPv6), which expands the number of users/addresses that the network could accommodate. Therefore, the global power of Taiwan's ICT industry in terms of market leadership and innovation holds the key to unlock its potential to field one of the most advanced and cost- effective C4ISR infrastructures in the world.

C4ISR Modernization and Disaster Relief:

Taiwan's military has a tradition of responding to emergencies in support of civil authorities. However, the growing complexity of emergency management may mandate a review and possibly a new paradigm. In fact, adjustments may already be underway. In his national address on October 10, 2009, President Ma Ying-jeou highlighted that his administration has launched "reforms of current disaster preparedness systems and operations aimed at strengthening coordination and communications between central and local governments, training and drilling local government units in routine disaster preparedness measures, and heightening citizens' awareness of the importance of disaster preparedness."[60]

Advantageously, fundamental network centric operational concepts can also apply to disaster warning, recovery, and response. For example, emergency management centers for disaster warning and response, with fused sources of data and alert systems and command and control systems, could serve as viable backup military command centers at the central and local levels. Airborne command and control systems could also serve as emergency responders.

Sensors

Intelligence, surveillance, and reconnaissance (ISR) solutions could permit Taiwan's national security establishment to forecast security threats, maximize multi-domain situational

awareness, and "buy back" warning time to anticipate and respond to threats. Early warning is crucial to assess the nature of impending attack, alert the national leadership to enable them to determine the course of action, alert air defense forces and bases so aircraft can be flushed, ascertain rules of engagement, , and warn the civilian population.

As discussed, the negation of Taiwan's early warning capability would be considered critical to the success of any PLA campaign. Thus, a survivable network of sensors would be as important to the island's defense as would an individual's eyes, ears, touch, and smell in a time of crisis. Sensors used for natural disasters, border control, and pandemics have potential military applications that could be less expensive and perhaps just as capable. For pervasive and persistent surveillance, a network of low-cost sensors may be the key. Technological breakthroughs in the fields of nanotechnology and micro-electromechanical systems (MEMS) have driven costs down, due in large part to civilian market demand, which could lead to their adaptation for the C4ISR network.

Whether for reasons of economic security, environmental protection, space debris monitoring, island defense, counter-trafficking, or any combination of these reasons or others, maintaining awareness in all domains is a goal envisioned by most countries in the world. With this in mind, Taiwan may be a valuable partner in monitoring activities in the region in all domains, from deep under the ocean to the outer reaches of space.

Space Based Sensors for All-Hazards Preparedness

A space-based earth observation system consisting of electro-optical and synthetic aperture radar (SAR) remote sensing satellites could make a significant and cost-effective contribution to all-hazards preparedness. A combination of electro-optical and SAR satellite imaging is useful for all weather, day/night warning of potential dangers, as well as in disaster response. Satellites can provide information of damage, particularly when it is difficult to reach the affected area by land. In addition to accessibility, space imaging can also survey a larger area in a shorter amount of time than traditional ground cover study methods. Remote sensing by satellite can also forecast the expected spread of the disaster to other areas as well as provide vital information for search and rescue operations.[61]

Space-based sensors also support economic development, environmental protection, and military readiness. They are useful for efficient and effective land planning, monitoring of sea states, detection of landslides and undersea mudslides, flood mapping, and counter-trafficking. On the military side, satellites also are critical for assessing PRC capabilities and intentions and providing early warning of impending hostilities. Therefore, remote sensing satellites should be an essential part of any longer term cross-Strait peace process. If the two sides enter into some form of force reduction agreement, it would be critical for Taiwan to have its own independent means of verification. This is perhaps the most important strategic function of the sensors in peacetime.

In the event of a conflict, remote sensing satellites can be warfighting assets. However, they could also become the target of the PLA's proven ability to intercept and destroy satellites in low earth orbit. One measure to enhance the survivability of the space-based sensor system is to utilize an architecture of small satellites, preferably supported by a domestic space launch

program. In the past, Taiwan has had a program to launch mission-specific 100-kilogram satellites into an orbit of between 600 to 800-kilometers.[62]

Taiwan's Satellite Capabilities:

Taiwan currently operates a single remote sensing satellite – Formosat-2 – and procures commercial imagery from a number of foreign sources. Designed with a 2-meter spectral resolution and procured from France's Astrium, the Formosat-2 remote sensing satellite was launched on an Orbital Sciences Corporation launch vehicle from Vandenburg Air Force Base in California on May 20, 2004. French export control authorities imposed operational restrictions or "shutter controls" that limit the satellite's ability to image high interest areas. The satellite was designed to operate for five years, and is currently nearing the end of its operational life.[63]

The launch of Formosat-2

Source: EADS

Plans have been in place since 2004 to procure or develop follow-on electro-optical and a first generation SAR system. Alternate plans to acquire turnkey satellite systems have experienced prolonged delays due to funding shortfalls and anomalies in the procurement process. Other plans have included indigenous design and development of two earth observation systems, known as Formosat-5 and Formosat-6. The Formosat-5 is conceived as an electro-optical system that would replace the Formosat-2 satellite. According to Taiwan's National Space Office, the satellite is designed with a 2-meter resolution a five-year life. It is to be launched in 2013 into a sun synchronous orbit at an altitude of 720-kilometers.[64] The Formosat-6 is intended to be an indigenous 50-kilogram microsatellite to be launched on a domestic or other small launch vehicle in 2012.[65] However, both of these programs have experienced bureaucratic delays and funding inadequacies.[66] As a result, Taiwan will likely experience an extended delay in fielding a replacement, which could have applications in disaster response, economic planning, military preparedness, and arms control verification.

The successful deployment of Formosat-5, Formosat-6, or other remote sensing satellite could position Taiwan to contribute to international organizations established to pool resources for the purposes of emergency preparedness. One forum worth exploring is the Global Earth Observation System of Systems (GEOSS) project. As a United Nations project, GEOSS aims to pool all national and regional observation data by 2015 for scientific and economic purposes. The U.S. is also a participant in GEOSS through the Integrated Earth Observation System (IEOS).[67]

Taiwan has actively sought greater access to international resources for its own disaster preparedness efforts and has offered to contribute to the GEOSS community. In one program, Taiwan's National Science Council pooled the island's expertise to design and develop an innovative 3D geographic information system that leverages the remote sensing assets in order to support national-level disaster response. In June 2009, Taiwan sponsored an

Integrated Earth Observation System (TIEOS) Forum as part of its effort to play a more prominent role in the global remote sensing community.[68] Most recently, the National Aeronautics and Space Administration (NASA) credited Taiwan's Formosat-2 satellite for supporting disaster relief operations in the Honduras and Belize after an earthquake struck in May 2009.[69]

Airborne Sensors for All-Hazards Preparedness

Manned or unoccupied airborne sensors, such as unmanned aerial vehicles (UAVs) and airborne signals intelligence aircraft, are useful for a range of purposes, including: disaster warning; response, and recovery; border control and law enforcement; land planning; as well as military operations.

UAVs offer promising opportunities for constant surveillance of Taiwan's operational environment to meet non-traditional and military requirements. Relatively low cost UAVs could be fitted with many different types of sensor packages, including electro-optical, infrared, and SAR imaging payloads, as well as signals intelligence receivers. With their multiple launch options, UAVs could operate day and night to monitor maritime activity and, if required, provide targeting data for strike assets.

Integration of the various sub-systems, from the engine, airframe, control system, sensors, jam resistant high speed data links, to ground stations, may be the greatest challenge in fielding a low- cost, multi-purpose system. Logistically, a reliable airspace management system will also need to be established to avoid collisions with commercial airlines and fighter jets.

Despite their potential, current design and technology for UAVs are limited some aspects. Firstly, UAVs require a rather small antenna for downlinking collected data to ground stations, which is a limiting factor for the rate of transmissions. Surveillance UAVs, which transfer multi spectral data from infrared and ultraviolet sensors, take up a great deal of bandwidth, as do both regular definition and high-definition video.[70]

UAV programs in Taiwan to date include the Chungshan Institute of Science and Technology's (CSIST) UAV for the ROC Army, as well as prototypes developed by Cheng Kung University's Remotely Piloted Vehicle and Micro Satellite Research Lab (RMRL). While the CSIST's UAV program had experienced technological bottlenecks, presumably due to U.S. export licensing restrictions, the system is currently scheduled for early operational capability in 2011.[71]

Another option for airborne sensing is an airship that operates in the near space domain. Near space is defined by the Fédération Aéronautique Internationale (FAI) as the air and space boundary between 20 and 100-kilometers (65,000 to 328,000-feet) above ground. The near space realm is too high for fighter jets and even reconnaissance airframes, such as the SR-71, U-2, and Global Hawk, and too low for orbiting satellites. However, near space platforms offers several advantages, including coverage that is comparable to low orbit satellites with significant improvements in resolution. The flight duration these platforms are also close to those of satellites, far exceeding other reconnaissance apparatuses such as UAVs. Powered at least in part by light, high efficiency solar cells, near space vehicles (NSVs), such as airships, offer a relatively inexpensive means for persistent broad area surveillance that is impervious to weather conditions making it ideal for disaster preparedness and other contingencies. A

number of entities around the world are designing and developing commercial airships with multiple sensors, including SAR, electro-optical, electronic intelligence, and infrared amongst others vehicles.[72]

Surface-Based and Maritime Sensors for All-Hazards Preparedness

Space and airborne sensors can be augmented by a variety of surface-based and maritime sensors. Possibilities include additional radar systems for air and maritime surveillance, undersea arrays for monitoring earthquakes and volcanic activity, climate change, and border control, as well as passive sensors for air surveillance and other missions.

Taiwan has devoted significant resources into survivable early warning, air surveillance, and command and control. Notably, it invested almost U.S. $800 million in a long-range, large-phased array UHF early warning radar that is now being installed atop a high mountain in northern Taiwan. The early warning radar is designed to detect large numbers of ballistic and airbreathing targets at extended ranges. Like its PAVE PAWS predecessor, (a U.S. Air Force Space Command radar system), the radar also could track PRC satellites and support Taiwan's own satellites. Software restrictions on long range UHF early warning radar could be relaxed to give Taiwan a space tracking capability to assist in monitoring space debris; monitor PRC satellites to facilitate a concealment, camouflage, and deception program; and augment Taiwan's own space control, tracking, and telemetry network. As an early warning system, the radar is not expected to survive beyond the initial strikes in a full-scale assault. Therefore, Taiwan has also invested in other surveillance assets, including new radar systems operating in the L- and S-Band portions of the frequency spectrum. Taiwan also has spent more than U.S. $250 million to upgrade its air defense command and control system, which plays a central role in threat assessment and weapons allocation.[73]

Today, Taiwan has one of the world's most advanced early warning and surveillance networks. Nevertheless, air surveillance and control may be difficult to sustain in the face of a dedicated air defense suppression campaign. The PRC's procurement of anti-radiation missiles, jammers, and increasingly accurate and lethal ballistic and land-attack cruise missiles present survivability challenges. This threat warrants further examination of enhancing the effectiveness of the existing network or augmenting it with other capabilities. Taiwan could adopt passive ground-based sensors to augment conventional UHF, L-, S-, and X-Band radar systems that may be vulnerable to jamming or physical destruction. Passive coherent location (PCL) systems offer precise real-time, all-weather detection and tracking for air surveillance, missile tracking and homeland security applications. PCL systems can track targets at ranges of more than 120-kilometers within the field of view without generating a radiofrequency (RF) pulse.[74]

Based on commercial technology, passive sensors can be less costly to acquire, operate, and maintain than traditional radar systems. If Taiwan can capitalize on its global competitive advantage in advanced signal processing components, then PCL systems can present a viable option for bolstering its sensor infrastructure. Other options include infrared search and track (IRST) capabilities that can detect and monitor objects with heat signatures, such as aircraft and helicopters.[75]

Border Control and Maritime Security: Minding the Coastline, Coastal Waters, and Beyond

Another important security requirement for Taiwan is wide area surveillance that is capable of cooperative and non- cooperative tracking and detection in all domains. Authorities in Taiwan have begun to examine ways to ensure persistent surveillance of the island's 1566-kilometer coastal border.[76] As an island, its maritime borders need to be guarded against illegal immigration, drug trafficking, and other illicit smuggling activities. Beyond the coastlines, it is critical to ensure the security of maritime traffic and the country's fishing industry. Security measures could include coastal, undersea and over-the-horizon maritime surveillance assets, access to a common maritime traffic database and global air traffic control information, undersea surveillance assets, and digital maps and imagery.

In particular, over–the-horizon (OTH) radar systems, an undersea surveillance system, and mobile undersea sensors offer significant capabilities for all-hazards defense. First, high frequency OTH radar systems provide an affordable means of monitoring maritime activity at extended ranges. OTH radar signals beam off the ionosphere to a range of 2000 to 3000-kilometers allowing the system to monitor ocean currents and other sea state conditions for accurate typhoon warning and analysis.[77] The system can also fill a critical gap in regional security by tracking North Korean shipping and potential WMD-related cargo in the Western Pacific, Bashi Strait, and South China Sea. While the OTH system is a cost-effective solution for a range of security challenges, it requires a two to three-kilometer area to deploy an array. However, once deployed, the OTH radar system could fill a vital gap in maritime domain awareness.

Secondly, an integrated undersea surveillance system could be a key component of an all-hazards situational awareness network. Among the civilian uses include the monitoring of earthquakes, tsunamis, volcanic activity, oceanographic research, and fish migrations. Underwater arrays could function as stealthy assets for the purposes of maritime surveillance in support of counter-trafficking and border control. Undersea surveillance devices could also be useful for the strategic cueing of airborne and other anti-submarine warfare assets. Harbor surveillance apparatuses could facilitate the detection of underwater swimmers, explosives, and mines. Underwater arrays could also contribute to the regional Deep-Ocean Assessment and Reporting of Tsunami (DART) program managed by .the U.S. National Oceanic and Atmospheric Administration (NOAA).[78]

Finally, mobile undersea sensors in the form of small submarines can heighten situational awareness. Their stealth and ability to remain on station for long periods of time can often foil an adversary's attempt to deny or deceive intelligence collection efforts. As a major component of an integrated signals intelligence architecture, submarines are able to discreetly monitor line-of-sight transmissions. The strategic benefits of the situational awareness mission alone merit the design, development, and production of small, cost effective submarines. For non-military missions, submarines are useful for scientific research and counter-trafficking. Taiwan can follow Australia's example of employing small submarines for harbor defense and counter-drug trafficking operations.[79]

Communications

Attacks on government communications systems can accelerate breakdown of political and military by reducing direct communication from the strategic (civilian) to theater level operations. The loss of communications at the theatre level presents a severe challenge for coordinating critical logistics, firepower, communications, electronic warfare, intelligence, and deception. Similarly, strikes against the military communications system can force airbases and other tactical units to operate autonomously or on localized information during a national crisis. Furthermore, disruption of strategic communications would impede the ability of the Taiwan's national political leadership to reassure the population or to orchestrate civil support for military operations.

The range of possible attacks on the communication systems extend beyond jammers. Critical nodes in the wireless communication network can also be targeted. A wireless system, such as a mobile cellular network, is typically partitioned into regional cells and each cell is serviced by a base station that is connected to the network via a mobile switching center. Each cell is serviced by a base station connected to the network via a mobile switching center. The loss of a mobile switching center, whether through physical destruction, loss of power supplies, or interruption of its computer systems, could affect wireless communications across a broad area.[80]

However, the PLA is not the only threat to Taiwan's telecommunications infrastructure. When a natural disaster or other emergency occurs, the communications infrastructure is often one of the first casualties. During emergency situations, use of the telecommunications expands significantly and can overload the system's capacity. Problematically, emergency situations are also times when reliable communication is most needed for effective disaster warning, response, and recovery. For mass casualties, telemedicine would be critical, which in turn requires a reliable means of communication.[81]

The most significant awakening to the fragility of Taiwan's communications infrastructure was the September 1999 earthquake. The earthquake caused a breakage in the primary backbone cable that spans the perimeter of the island, a rupture in an undersea cable, collapse of cell sites and radio relays, and caused extended power outages in key communication facilities. While the extensive damage hindered emergency responses, it also demonstrated the necessity of bolstering communications in disaster relief planning.[82]

Challenges in Improving the Communications Network:

Taiwan may be home to the densest RF environment in the world, given the high concentration of radar systems, cell phone and other wireless networks, and other emitters. Among the systems operating in Taiwan include AM and FM radios, short-wave and citizens' bands, VHF and UHF television channels, as well as hundreds of less familiar bands that serve cellular and cordless telephones, GPS trackers, and air traffic control radars. The high concentration of systems could render densely populated areas vulnerable in an emergency as responders will have to navigate frequency management and possible RF fratricide concerns.

Another challenge is the lack of interoperability between different government bureaucracies on the island, and within the defense establishment. Taiwan's Po Sheng program is one initial effort to establish a common interoperable communication standard. Spanning a much smaller territory, Taiwan has the potential to further develop a viable interoperable network, perhaps drawing upon Sweden's successful civil-military C4ISR integration, and could serve as an international model for best practices.[83]

A final challenge Taiwan faces is its limited lines of communication to the outside world. Approximately 95% of the international communications traffic travels by undersea cable, with the rest via satellite. However, Taiwan possesses only a handful of undersea spurs running off major regional trunk lines and a few satellite ground stations. The vulnerability of Taiwan's buried or undersea cable has in part driven the development of wireless communications.

Both despite and because of these challenges, Taiwan has the potential to be the world leader in communication preparedness in the most stressing of scenarios. Given its central role in the global information and communications technology supply chain, even low-cost solutions could save countless lives, prevent further damage, and assist in the most effective response possible. Taiwan could also use its indigenous advantages to undertake collaborative efforts with other countries seeking to advance their own communications capabilities. Potential partners include the U.S., which could benefit from experiences in effective use of the RF spectrum and responding to threats that simulate PRC attacks or an electronic warfare campaign. The resultant lessons and technology could inform U.S. emergency management systems plans and programs.

Looking beyond the major existing programs, such as advanced tactical data links, Taiwan has a variety of options for enhancing communications in a crisis situation. These include leveraging civilian technologies for military applications, using interoperable civil-military networks, micro-terminal satellite systems and satellite digital audio broadcasting, software-defined and cognitive radios, internet protocol (IP)-based communications, ultra-wideband radios, and UAV-based communications relay.[84] Because bandwidth in Taiwan is a highly valued resource, there is a general trend is toward broadband wireless systems with advanced bandwidth sharing properties.[85]

Communication Systems: Wireless Networks, Cable and Satellite Communications:

A discussion of communications systems supporting emergency response operations could be divided into: 1) wireless networks; 2) cable; and 3) satellite communications.

Wireless Communications Networks. Wireless networks, including radios and cell phone networks, are a key area of investment. Wireless systems rely on the transmission of signals within the atmosphere. One of the challenges of wireless communications is managing the finite RF spectrum despite growing demand for cellular telephones, land-mobile radios, commercial broadcasting, and other RF applications. Taiwan has a number of programs intended to increase available bandwidth and connection speed, enhance military capabilities, and respond to natural disasters as well as other contingencies.

Other Wireless Tactical Communications Programs. Taiwan's advanced tactical data link system represents a revolutionary shift within the island's traditionally hierarchical and centralized command and control system. While JTIDS-like advanced tactical data links are important, Taiwan has a number of other wireless tactical communications programs. An example is the Enhanced Position Location and Reporting System (EPLRS) data links (425 to 427-MHz at 2.45 kbps) which have been used by the U.S. Army for many years, and one modified variant used by the U.S. Air National Guard is considered to be a low-cost alternative.

In the near term, Taiwan's defense establishment appears to be preparing for at least three radio programs managed by the Army, Navy, and Air Force. An example is the existing Improved Mobile Subscriber Equipment (IMSE) systems and PRC-37A frequency-hopping VHF radio. For strategic and operational-level communications, long-standing plans have been in place to develop and install a modern HF network. The network is supposedly intended to support the Hengshan National Command Center for emergency presidential-level communications. It also was intended to link together major service headquarters, the Air Operations Command, and Taiwan's two primary naval task forces (the ROC Army's Special Operations Command, the Marine Corps Command), and the four major offshore island territorial defense commands.[86] In addition to facilitating military coordination, the network will support civilian emergency response. The ROC Air Force is also seeking to modernize its air-ground communications through the procurement of as many as 179 new VHF radios.[87]

As a final note, development and improvements upon military radios have also been relatively slow in comparison to their commercial counterparts. Commercial advances in other wireless technology have approached military systems in terms of bandwidth, speed, and quality of service. Taiwan's ongoing Worldwide Interoperability for Microwave Access (WiMAX) program holds potential for integrating civil and military systems. WiMAX can transmit volumes of information at a range of 50-kilometers using stationary line of sight communications (5 to 8-kilometers for mobile users) and can support data rates of 50 kilobits per second or more. Taiwan, second only to the United States, is the largest investor in this kind of communications infrastructure.[88] The U.S. Army is also evaluating the implications of WiMAX for its own use.[89]

Associated with its WiMAX program, Taiwan also has been touted as a leader in designing, developing, and producing an ultra-mobile PC (UMPC) that integrates sophisticated computing with a communications device. Known as "M-Tube," the system was designed for use in conjunction with the WiMAX network. With short battery life being the primary drawback, the 2.8-inch screen device is driven by a rapid GHz-level processor and weighs mere 150-grams.[90]

Software Defined Radios. As global military trends shift toward the use of configurable communication systems, a software defined radio (SDR) offers another wireless solution. The SDR device uses software instead of hardware to perform all of its signal processing and applications thus allowing a single communications device to interoperate with many different wireless systems. The pilot program for a software communications architecture and SDR is the aforementioned DoD JTRS program, which intends to replace as many as 25 different radio systems in the DoD inventory with a single standard for all radio systems. Since multiple functions of a communications device can be incorporated into a single radio, an SDR can be upgraded to enable new standards and services. As a result, the life cycle costs associated

with software-defined communications architecture are significantly less than legacy systems.[91]

The heart of a SDR is its digital signal processors (DSP) that reconfigures the various waveforms. Taiwan has been the principle global supplier of state of the art microelectronics, such as Field Programmable Gate Array (FPGA) sized at 65 nanometers and below, with applications in JTRS and other SDRs.[92] However, Taiwan's position at the cutting edge of the defense information revolution transcends tactical radio systems. To quote a senior DoD engineer, "the majority of the ICs [integrated circuits] used in complex modern military systems are made off-shore. FPGAs are the dominant IC used in modern weapons systems, and all FPGAs are made off shore.[93] Taiwan is estimated to supply up to 80% of the FPGAs used in U.S. information, communications, and weapon systems today. This reliance has raised concerns over the integrity of FPGA and other ICs which led to a Pentagon vulnerability assessment, establishment of cooperative programs with U.S. industry and presumably their contract manufacturers in Taiwan, as well as a rigorous anti-tampering program.[94]

Beyond JTRS and Software Defined Radios: Cognitive Radios. With one of the world's densest RF environments, one possible solution for efficient use of the limited frequency spectrum could be cognitive radios. Cognitive radios are one component of mobile ad hoc networks (MANET). Taiwan's research and development community has begun serious investigation into the applicability of cognitive radio networks for emergency response missions.[95] Cognitive radios, with their ability to automatically reconfigure during intense interference, are able to establish communications networks at disaster sites when communications, electrical systems and even physical buildings are in disarray. The radios can sense the RF environment, adjust power, frequency, modulation, and even bounce the signal off buildings and rubble. In a military context, cognitive radios may be able to detect PLA enemy jamming or other RF interference and switch to unaffected frequencies.[96] Other communications technologies, such as ultra-wideband (UWB) systems, have also drawn attention. Using low amounts of power spread over a broad portion of the frequency spectrum, UWB systems may offer another means of survivable tactical communications.[97]

Landline/Cable Systems. In addition to wireless communication networks, Taiwan has strived to upgrade its underground cable backbone networks. A major program to expand the capacity of the military information and communication system (MICS) and its integration with the civil national information infrastructure was reportedly completed in 2004. The MICS ostensibly connects all joint and Service-level command and intelligence centers to a portion of Taiwan's operational forces through new ATDLS tactical data link remote radio sites. Taiwan's new command and control system was also intended to leverage upgrades to the MICS to integrate various sensor data, including signals intelligence, imagery, and streaming video from terrestrial, airborne and space platforms into a common operational picture.[98]

Terrestrial-based infrastructures, whether wireless or wired, are inherently vulnerable due to their requirement for physical structures. Most communication pathways linking Taiwan with the rest of the world are routed through one of two ways – via undersea cable or satellite ground stations. Submarine or undersea cables are particularly exposed to disruption from both man-made and natural hazards.[99] Undersea cable networks connecting Taiwan to the region are spurs or branches to major links. These spurs and branches, or their landing points in the greater Taipei and Kaohsiung, are critical points of failure that could isolate Taiwan's communications from the international community. A RAND study noted that four of five

undersea cables reaching Taiwan land at one of two sites (Toucheng and Fangshan). Damage to these cables could stress Taiwan's ability to communicate with the outside world since all traffic would have to be routed through the island's limited satellite links.[100]

Taiwan's undersea cable network has proven to be fragile. A few years ago, a line rupture off the coast of Shanghai resulted in disruption of connections for three of Taiwan's main internet service providers (Hinet, Seednet, and TANet) with U.S. networks for several hours. More recently, the 7.1 magnitude Hengchun earthquake on December 26, 2006 ruptured cables off the cost of Kaohsiung and resulted in one of the largest disruptions of modern telecommunications systems in history. The earthquake set off a chain of events, including an undersea landslide, which damaged nine submarine cables in the Bashi Strait.[101] During Typhoon Morakot in 2009, six undersea internet and communications cables carrying traffic throughout Asia were severed or damaged.[102]

Satellite Communications. Communications systems that rely on ground-based nodes have the potential to fail when needed most. For that reason, satellite communications may offer a critical lifeline during natural disasters and other emergencies. In the event of a catastrophic failure of land-based systems, satellite communications could link fixed command centers, mobile assets, or broadcast emergency information with a wide array of users. The requirement for dedicated emergency response satellite communications was evident during the Typhoon Morakot recovery effort when the PRC's China Mobile company responded to Taiwan's needs by providing three mobile satellite base stations.[103]

Currently, Taiwan's satellite communications infrastructure relies exclusively on external service providers. For the bulk of the island's satellite communications, Taiwan's Chunghwa Telecom rents transponder space on Singapore Telecommunication's ST-1 satellite. Built at a cost of US $240 million, the C/$K_u$-Band satellite was launched in 1998 and is expected to end its operational life around 2013. However, Taiwan and Singapore have reportedly agreed to cooperate on a second satellite, ST-2, which is planned for launch in late 2010.[104]

Designed to operate in the K_u-band portion of the frequency spectrum, the ST-2 is expected to share the shortcomings of the existing system. Satellites operating in the C/K_u-band portion of frequency spectrum have bandwidth limitations and are subject to interference through the use of ground-based jammers. As an example, indications exist that the PRC jammed ST-1 broadcasts in the run-up to October 1st national day celebrations in 2009.[105] However, the increasing availability of anti-jam capabilities offered by U.S. companies may present some degree of security through beam-forming technologies and frequency hopping and spread spectrum modems.[106]

Broadband communication satellites, operating at higher frequencies than K_u-Band, often using mini-satellite terminals small enough to fit in the palm of one's hand, have become an option for many telecommunications providers around the world. Japan recently launched such a broadband communication satellite, Kizuna, which offers high-speed internet access throughout the country and the region without the need for terrestrial infrastructure. Through a small antenna and a direct view to the southern horizon, users can download data at 155 mbps and upload at 6 mbps. Built by Mitsubishi Heavy Industries at a cost of U.S. $485 million, the system has direct applications for personal use, for backing up terrestrial networks in an emergency, and for emergency medical care in remote areas.[107]

While Taiwan does leverage other mobile satellite services, the investment with greatest returns in a crisis situation may be in an ROC-owned and operated broadband communications satellite.[108] From the late 1990s until the early 2000s, Taiwan considered procuring a dedicated broadband (K_a-Band) communications satellite that would have offered a high degree of security, and direct connectivity with the international community. As a centerpiece of the original Po Sheng program, it was envisioned that the broadband communications satellite would be linked to more than 350 small satellite terminals.[109]

One interim option evaluated by DoD is the use of commercial satellite radio for emergency broadcast purposes. DoD, as part of its series of joint experiments, has favorably tested satellite radio systems, such as XM Radio, for military and homeland security applications. The program, entitled Mobile Enhanced Situational Awareness (MESA), is an inexpensive data-casting suite that passes situational awareness information such as map and entity data globally or individually to warfighters using commercial narrowband satellites, such as those used by XM satellite radio.[110] Satellite radio is now being used for emergency management services, ranging from tsunami warning to disaster response and recovery, around the world. For Taiwan, access to or management of an indigenous satellite radio system would not only ensure contact with international emergency broadcast and communications services, but could also enhance its international stature and global mindset through dozens of channels of radio broadcasting.[111]

Command and Control

Communications are the glue that binds Taiwan's strategic and operational-level command and control structure with fielded military forces and emergency response assets. An effective and survivable command and control system is the most fundamental requirement of emergency operations. In the absence of an effective command, a military organization – or any another emergency response system - is little more than rabble. Destruction or paralysis at any level of command can have serious or fatal effects on its subordinate elements. In a conflict, the key challenge for the opponent is locating the critical command facilities that contain not only the commander, but also perhaps more importantly, the staff supporting the conduct of military operations.

As an open and democratic society, Taiwan's chain of command and organization have become the topic of widespread media coverage. Taiwan's supreme commander in an emergency is the President, who directs operational forces through the Minister of Defense. Facilities playing a leading role include the Hengshan command center (衡山指揮所), a newly established civilian center in Yuanshan, a disaster response command center in Sanchung [Central Emergency Operations Center; 中央災害應變中心], and a health-related command center. Press reports note that Hengshan also houses the Tri-Service Command, and the Hengshan Command and Control System.[112] Since 2006, Taiwan has also established city and county-level disaster response centers.[113]

Taiwan's emergency management system has evolved over the years as potentially one of the world's most advanced. This began with a departure from its traditional approach of a stovepiped command and control system. Since 1999, Taiwan has implemented a range of measures to plan for emergency responses, including the establishment of a central disaster

prevention and response council, the drafting of national and local level contingency plans, and the formation of emergency response command centers at both the national and county/city level. Furthermore, government departments have been delegated responsibility for various types of disasters. For example, the Ministry of Interior has responsibility for earthquakes and typhoons, and the Ministry of Economic Affairs is responsible for floods and critical infrastructure protection.

Agencies responsible for emergency management operate individual command and control centers. For natural disasters, once the Central Weather Bureau (CWB) issues a warning, Taiwan's Central Emergency Operational Center (CEOC) is activated and transmits analysis to various government agencies. Representatives from other disaster-related agencies will also staff the CEOC.[114] Taiwan's National Health Command Center (NHCC), the command post of the CDC, is responsible for preparedness, surveillance, and response to epidemics and pandemics.[115] The National Fire Agency (NFA) is the primary organization responsible for rescue and relief operations. However, Taiwan's senior political leadership has been evaluating changes to the island's natural disaster response organization and procedures, drawing heavily from Japan's experiences. According to sources in Taipei, plans may include formation of a specialized emergency response organization directly subordinate to the President's Office.[116]

Operational Command and Control:

Adjustments also have been made to Taiwan's military command and control system. In addition to upgrades to Taiwan's national and operational-level command and control system covered under the Po Sheng program, Taiwan has invested more than U.S. $250 million in upgrades for its air defense command and control system that would be responsible for threat assessment and weapons allocation.[117]

Taiwan has also taken steps to enhance its maritime surface and underwater surveillance system. However, perhaps the most significant area of potential investment is in an upgraded command and control system (known as Ta-Chen) and integration of sensors. As it new maritime patrol aircraft and other ASW surveillance assets enter Taiwan's operational inventory, the importance of fielding an ASW operations center (ASWOC) should grow. Expanding the number of ships in Taiwan's advance tactical data link network, including the PFG-2 destroyers, Lafayette frigates, and fast attack boats, would create greater synergies between the Navy and with other services, as would integrating the Ta-Chen command and control system with the Po Sheng network.

Another option for command and control is a capability known as maritime domain awareness (MDA). A multi-dimensional awareness capability could integrate existing and future radar systems, including OTH systems; advanced information systems; imagery and video; acoustic data; beacons, and information drawn from global data bases, such as Lloyd's ship registry.[118] Command and control system upgrades under Po Sheng are said to incorporate capabilities similar to those used in U.S. MDA-related harbor surveillance programs.[119]

Taiwan's emergency response command and control system, military and otherwise, could derive significant benefits from cost effective data fusion and visualization systems, as

exemplified by MDA. Such a capability largely depends on a user-friendly and affordable software package that is capable of fusing or correlating a wide variety of sensors. Ideally, the software will allow satellite imagery, three-dimensional terrain maps, and live video and radar feeds to be displayed on high-resolution monitors.[120] Furthermore, Taiwan could be a good candidate for participation in a global MDA system. It could contribute its coastal and OTH tracking of cooperative and non-cooperative shipping on the high seas. Access to a global MDA database could allow Taiwan to fuse its own surveillance with data bases describing the nature of all ships operating near Taiwan in the Western Pacific Ocean and transiting through the Bashi Channel, perhaps the busiest sea lane in the world. [121]

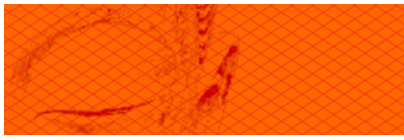
Conclusion

As the cognitive and central nervous system coordinates an individual's sensory and response mechanisms, a country's C4ISR capabilities are essential for situational awareness and communication in times of emergency. As with individuals, this ability is often taken for granted until lost or faced with a severe failure. C4ISR is fundamental to both modern warfare and crisis response. While C4ISR alone will neither destroy an adversary target nor accomplish emergency resupply, none other activity in military operations is more important. With the advent of the technology revolution, there are increasing possibilities to fortifying critical C4ISR abilities.

At the forefront of the global information revolution, Taiwan is yet to leverage its technological and innovation advantages for its defense and non-traditional security. However, faced with some of the world's most stressing security challenges, Taiwan is investing greater resources into resilient networks of sensors, communications systems, and command systems in order to better manage a range of emergencies. As a result, it has the potential to field one of the world's most advanced and networked C4ISR systems.

However, there is more that could be done. Promising steps include expanding the number of participants in Taiwan's advanced tactical data link system to increase its network centric operations capability. Further enhancements to its command and control system, especially to support ASW operations, would better prepare the island's civil and military leadership for emergency management. Cultivating innovation in its defense establishment, perhaps drawing upon Singapore's Future Systems Directorate as an example, would help generate ideas and unique solutions to Taiwan's challenges.[122] Going forward, Taiwan should examine theories and international experiences in civil-military integration and adapting commercial technology to enhance efficiency in use of limited resources.[123]

Furthermore, all-hazards C4ISR should be a strategic priority in U.S.-Taiwan relations. The United States offers a number of experiences that could be applied to Taiwan's unique situation, while Taiwan may offer insights into areas in which it has excelled. A joint assessment team could evaluate the benefits of adding a space tracking capability for Taiwan's UHF long range early warning radar, and possible military uses of advanced technologies and systems such as WiMAX, MANET, and other networks. In addition, the U.S. and Taiwan could consider joint design and development projects associated with maritime OTH radar systems, integrated undersea surveillance, and multi-purpose underwater vehicles for civilian and military purposes.



Blank page

References

[1] Bruce Einhorn, "Why Taiwan Matters," *Business Weekly*, May 16, 2005, at http://www.businessweek.com/magazine/content/05_20/b3933011.htm, accessed on December 1, 2009.

[2] Wang Houying and Zhang Xingye, *Zhanyixue* [Campaign Studies], Beijing: NDU Press, 2000, pp. 168-170.

[3] Yu Guohua, *Xiandai jingong zhanyi zhuyao wenti yanjiu* [A study on modern offensive campaigns], Beijing: NDU Press, 1999, pp. 69-72. The command system is referred to as the "vital point" (*yaoxue*; 要穴) of the enemy's entire operational system, consists of policymakers at the strategic level, the operational military command, and supporting command, control, and communications systems.

[4] For a general reference, see *Electronic Warfare*, Joint Publication 3-13.1, January 25, 2007, at http://ftp.fas.org/irp/doddir/dod/jp3-13-1.pdf, accessed on November 10, 2009.

[5] Quote drawn from James Mulvenon, "The PLA And Information Warfare," in James C. Mulvenon and Richard Yang, eds, *The People's Liberation Army in the Information Age* (Santa Monica, CA: RAND, 1999), p. 179.

[6] See Zhang Youcai, "Denglu zhanyi dianzi duikang zuozhan zhidao de jige wenti" [Some questions surrounding ECM operational principles during a landing campaign], in *Zuozhan zhihui yanjiu* [Research on operational command and control], Beijing: NDU Press, January 1997, pp. 327-333. Also see Zhang Chenhui and Cai Shichuan, "Jianli denglu zhanyi dianzi duikang zhihui xitong de tantao" [Discussion On Establishing An ECM Command System During Landing Campaign], in *Zuozhan zhihui yanjiu*, pp. 342-347; Wang Yongsheng, "Denglu zuozhan kongzhong jingong zhanyi de dianzi jingong xingdong" [Electronic Attack Activity During The Air Attack Campaign Of A Landing Operation], in *Gaojishu tiaojianxia zuozhan zhihui yanjiu*, February 1996, pp. 361-365; and Cui Yansong, "Kongjun zuozhanzhong de xinxizhan qianshen" [Survey of Information Warfare In Air Force Operations], in *Wojun xinxizhan wenti yanjiu* [Research on problems in PLA information warfare], Beijing: Guofang Daxue Chubanshe, p. 166-171.

[7] Wang Yongsheng, pp. 361-365.

[8] For examples of PRC studies on jamming JTIDS, see Liu Zhiguo and Zhao Xinguo, "Research on Characteristics and Jamming Methods of JTIDS," [JTIDS 链路特点及干扰方法初探], *Journal of the Academy of Equipment Command & Technology*, [装备指挥技术学院学报], Vol. 18, No. 1, (Feb 2007), pp. 79-82. Also see Wang Bangrong, Li Hui, Zhang An, and Zeng Wei, "Status quo and Future Development Trend of Tactical Data Links" [战术数据链的现状及未来发展趋势], *Fire Control and Command Control*, Vo1. 32, No. 12 (December 2007), pp. 5-9; and Yan Jiangang and Fan Yan, "Anti-Jamming Performance Evaluation of Link-16 Tactical Data Link System and its Simulation" [Link-16 战术数据链抗干扰性能评估与仿真], *Fire Control and Command Control*, Vol. 34, No. 2 (February 2009). For reference to use of high power microwave devices, see Wen Guangjun, Li Shigun, Guo Weili, Li Jiayin, and Li Lemin, "Study on the Possibility of Jamming JTIDS Signal with High Power Microwave Source" [高功率微波源干扰 JTIDS 信号的可能性分析], *Journal Of Sichuan Institute Of Light Industry And Chemical Technology*, Vol. 19, No. 3, (1999).

[9] Cui Yansong, "Kongjun zuozhanzhong de xinxizhan qianshen" [Survey of Information Warfare In Air Force Operations], in *Wojun xinxizhan wenti yanjiu* [Research on problems in PLA information warfare], Beijing: Guofang Daxue Chubanshe, 1999, p. 170.

[10] Ibid.

[11] Zhu Wenquan and Chen Taiyi, *Xinxi zuozhan* [Information Operations], Beijing: NDU Press, 1999, p.75. Technical reconnaissance is known as *jishu zhencha* (技术侦察) or *jizhen* (技侦) for short, a euphemism for signals intelligence.

[12] Since the mid-1990s, the PRC is said to have received assistance from Russian scientists who are considered to be the leading experts in the world on nuclear and non-nuclear radiofrequency weapons.

[13] For detailed discussion of HPM systems, see Mark A. Stokes, *China's* Strategic Modernization*: Implications for the United States* (Carlisle, PA: Strategic Studies Institute, 1999). Also see Lin Zheng, "New Advances in Electronic Warfare," in *Proceedings of '96 Conference Sponsored By "Huoli Yu Zhihui Congzhi" Journal,* October 1996, pp. 16-21, in *FBIS-CST*-97-012; Zhang Zhenzhou, "Longitudinal Tranmission of Exploding Electromagnetic Waves," *Xiandai Fangyu Jishu*, April 1995, pp. 47-58, in *CAMA*, Vol. 2, No. 5. Also see Qin Zhiyuan, "HPM Weapons in Tomorrow's War," paper presented at 1997 COSTIND sponsored international conference on RMA. For reference to use of HPM devices to counter JTIDS, see Wen Guangjun, Li Shigun, Guo Weili, Li Jiayin, and Li Lemin, "Study on the Possibility of Jamming JTIDS Signal with High Power Microwave Source" [高功率微波源干扰 JTIDS 信号的可能性分析], *Journal Of Sichuan Institute Of Light Industry And Chemical Technology*, Vol. 19, No. 3, (1999). For use of HPM to neutralize SATCOM, see Zhou Jiabo, "Exploration of Space Communications Countermeasures" [空间信息对抗初探], *Radar and Electronic Warfare* [雷达与电子战], January 2007, pp. 7-14.

[14] For a comprehensive overview of HPM technology and potential application, see Carlo Kopp, "The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction," *Chronicles Online Journal* (U.S. Air Force) October 1996*,* at http://www.airpower.maxwell.af.mil/airchronicles/cc/apjemp.html*,* accessed on January 20, 2010.

[15] For an excellent summary on the potential effects of a HEMP burst in a Taiwan scenario, see Chung Chien, "High Tech War Preparation of the PLA: Taking Taiwan Without Bloodshed," *Taiwan Defense Affairs*, October 2000, pp. 141-163.

[16] *The Military Power of the People's Republic of China: A Report to Congress*, (Washington DC: Office of the Secretary of Defense), 2005, at http://www.defense.gov/news/Jul2005/d20050719china.pdf, accessed on December 12, 2009, p. 40.

[17] For a good summary of a HEMP burst in a Taiwan scenario, see Chung Chien*,* "High Tech War Preparation of the PLA: Taking Taiwan without Bloodshed," *Taiwan Defense Affairs*, October 2000, pp. 141-163.

[18] For the Congressionally mandated report and an excellent overview of Chinese computer network operations, see Bryan Krekel, et.al., *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman Corporation Report, Prepared for The US-China Economic and Security Review Commission, October 9, 2009, at http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf, accessed on December 3, 2009.

[19] The attacks resulted in significant governmental, economic, and social disruption. While there have been large-scale denial-of-service attacks before, this is said to have been was the first time that such attack was directed against a nation, and it likely would not be the last. Speculation continues as to the source of attack, but Estonia insists that Russia - or Russian patriots - initiated the flood. For background, see "A Cyber-Riot," *The Economist*, May 10, 2007.

[20] For background on Taiwan's National Computer Emergency Response Team, see its website at http://www.twncert.org.tw/edex.aspx. For an early discussion of using information warfare as an asymmetric strategy, see Lee Wen-chung, "Taiwan's National Defense Construction in the Information Warfare Age," *Taiwan Defense Affairs*, No. 1, October 2000, pp. 148-156. Also see "Joint C4ISR Capabilities," *Quadrennial Defense Review* (2009), ROC Ministry of National Defense, March 2009, pp. 116-152, at http://www.mnd.gov.tw/QDR/file/ec4.pdf, accessed on January 3, 2010.

[21] Mark Stokes, "The Chinese Joint Aerospace Campaign: Strategy, Doctrine, And Force Modernization," in James Mulvenon and David Finkelstein, *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army*, (Alexandria: The CNA Corporation), December 2005, p. 265.

[22] This discussion is drawn from Wang Jianghuai and Zhu Guolin, *Gaojishu tiaojianxia hetong zhanyi hong/lan liangjun shouzhang jiguan duikang yanxi jiaocheng* [Lecture On Combined Red/Blue Campaign Command Organization Countermeasures Exercise], Beijing: NDU Press, 1997, pp. 104-110. Also see "ECM, Mobile Radar Units Integrated" [电子对抗、机动雷达分队混编(空军)], *Tengxun News Network*, September 28, 2009, at http://news.qq.com/a/20090928/001793.htm, accessed December 1, 2009.

[23] "A Certain Regiment in the Nanjing Military Region Advances New Operations and Training Doctrine" [南京军区某团改进新装备战法训法], *PLA Daily* [解放军报], July 10, 2009, at http://news.mod.gov.cn/forces/2009-07/10/content_4036016.htm. The Beijing Military Region ECM Regiment [66018 部队] is said to be near Changping [昌平]; the Guangzhou MR ECM Regiment [75737 部队] is located in the Huadu district; the Jinan Military Region ECM unit [71799 部队] is located in Zibo; Chengdu MR ECM Regiment [77108 部队] is near Chongzhou, west of Chengdu; the Shenyang MR ECM unit [65041 部队] is located in Sujiatun [苏家屯].

[24] "PLA Plans to Develop Army Aviation Units," *Sing tao jih pao*, October 22, 1999, p. A17 (FBIS: FTS19991028000246).

[25] Military Power of the People's Republic of China 2009, Annual Report To Congress, *Pursuant to the National Defense Authorization Act, Fiscal Year 2000,* March 2008, p. 27.

The PLA GAD allocates funding for and coordinates defense industry research and development of electronic warfare systems. The two entities responsible for electronic warfare systems are the China Electronics Technology Corporation's 36th Research Institute is also known as the Jiangnan Institute of Electronics and Communications [江南电子通信研究所] in Jiaxing (Zhejiang province) and the Southwest Institute of Electronic Equipment (SWIEE; or 29th Research Institute) in Chengdu. The 36th Research Institute's primary focus is on communications jammers and hosts a key PLA R&D lab on communications countermeasures [通信对抗技术国防科技重点实验室]. The 29th Research Institute focuses on radar jamming and hosts a general ECM laboratory [电子对抗国防科技重点实验室].

[26] Tim Culpan, "Taiwan's Major Threat Is Nature, Not China, President Ma Says," *Bloomberg*, August 18, 2009, at http://www.bloomberg.com/apps/news?pid=20601080&sid=awoSlB5BBgPk, accessed on November 21, 2009.

[27] Maxx Dilley, Robert S. Chen, Uwe Deichmann, Arthur L. Lerner-Lam, and Margaret Arnold, Natural Disaster Hotspots: A Global Risk Analysis, (Washington DC: World Bank Publications, 2005).[27]

[28] See Ben Jong-Dao Jou, "The Improvement of Emergency Operation and System Framework on Typhoon in Taiwan," paper presented at International Workshop on Emergency Response and Rescue, October 31-November 1, 2005.

[29] See "UN Report on Typhoon Morakot" [联合国公布第一号莫拉克台风情势报告], *United Daily News*, August 20, August 2009, at http://udn.com/NEWS/NATIONAL/BREAKINGNEWS1/5089937.shtml. In 2000 seven typhoons (Kaitak, Bilis, Prapiroon, Bopha, Yagi, Xangsane, and Bebinca) ravaged Taiwan, the most severe being Xangsane that resulted in 64 deaths.

[30] Chung-Ming Liu et al., "Climate Change Trends, Impacts, Vulnerability Assessment and Adaptation Measures in Taiwan: A Status Report," Global Change Research Center report, National Taiwan University, 2009 at http://climate.cier.edu.tw/upload/File/1006-en.pdf, accessed on December 7, 2009.

[31] "Opening Address of President Ma Ying-jeou at the European Union Climate Change Exhibition on the Campus of National Sun Yat-sen University," Presidential Office News Release, November 13, 2009, at http://www.president.gov.tw/en/prog/news_release/document_content.php?id=1105500082&pre_id=1105500082&g_category_number=145&category_number_2=145, accessed on December 18, 2009.

[32] Chintu Lai, Ting-Kuei Tsay, Chen-Ho Chien, and I-Ling Wu, "Real-time Flood Forecasting," *American Scientist*, Vol. 97, no. 2, Mar-Apr 2009, pp. 119-125. To the authors, "when geography teachers instruct their students about the great rivers of the world, the Amazon, Nile, Yangtze, Mississippi and Yellow usually head the list. Those are truly large rivers, but they earn their distinction by length. From a hydraulic engineer's perspective, however, neither length nor even total discharge is the most important characteristic. When it comes to flood

control and prediction, peak discharge per unit area of watershed (specific peak discharge) is the essential criterion, because it describes a river's volatility.

[33] Ibid.

[34] W.K. Hsu, D. M. Hung, W. L. Chiang, C. P. Tseng, and C. H. Tsai, "Catastrophe Risk Modeling And Application-Risk Assessment For Taiwan Residential Earthquake Insurance Pool, Proceedings of the 17th International Association of Science and Technology for Development (IASTED) International Conference on Modeling and Simulation, 2006.

[35] This assertion is based on US Geological Survey estimates.

[36] Tso-Ren Wu and Hui-Chuan Huang, "Modeling Tsunami Hazards From Manila Trench to Taiwan," *Journal of Asian Earth Sciences*, Volume 36, Issue 1, September 4, 2009, pp. 21-28; and Masataka Ando and Cheng-Horng Lin, "Assessment of Potential Tsunami And Earthquake South Of Taiwan Along The Manila Trench Using The Seafloor Geodetic Technique," presented at the Pingtung Earthquake Workshop. November 23, 2007.

[37] ibid.

[38] Authoritative observers have noted that most influenza pandemics since 1850 have originated in China. Among various references, see James E. Hollenbeck, "An Avian Connection as a Catalyst to the 1918-1919 Influenza Pandemic," *International Journal of Medical Sciences*, February 2005, pp. 87-90, at http://www.medsci.org/v02p0087.htm, accessed on September 8, 2009; and Robert G. Webster, "Predictions for Future Human Influenza Pandemics," *The Journal of Infectious Diseases* , Vol. 176, August 1997, pp. S14–19. Also see Laurie Garrett, "The Next Pandemic?," *Foreign Affairs*, July/August 2005. In this article, Laurie Garrett, a renowned global health specialist, argued that "if the relentlessly evolving virus becomes capable of human-to-human transmission, develops a power of contagion typical of human influenzas, and maintains its extraordinary virulence, humanity could well face a pandemic unlike any ever witnessed." She also writes that "aquatic flu viruses are more likely to pass into domestic animals -- and then into humans -- in China than anywhere else in the world."

[39] H. Chen et.al., "H5N1 Virus Outbreak In Migratory Waterfowl," *Nature*, Vol. 436, July 14, 2005; J. Liu et. Al., "Highly Pathogenic H5N1 Influenza Virus Infection in Migratory Birds," *Science,* August 19, 2005, Vol. 309, No. 5738, p. 1206; and Catherine Brahic,"China: Migrant Birds 'Open Flight Path For Bird Flu," *SciDevNet*, July 6, 2005.

[40] Hsieh Ying-Hen, "Excess Deaths and Immuno-protection during 1918–1920 Influenza Pandemic, Taiwan," *EID Journal*, Vol 15, No. 10, October 2009, at http://www.cdc.gov/eid/content/15/10/1617.htm, accessed October 28, 2009. The author is from China Medical University in Taichung.

[41] For a good summary of the potential effect of a pandemic on public services, see Utah Department of Health, *Governor's Taskforce on Pandemic Influenza Preparedness: Final Report to Governor*, Salt Lake City, Utah, April 2007.

[42] Utah Department of Health, *Governor's Taskforce on Pandemic Influenza Preparedness: Final Report to Governor*, Salt Lake City, Utah, April 2007.

[43] See, for example, Bruce Einhorn, "Why Taiwan Matters," *Business Week*, May 16, 2005; and Craig Addison, *Silicon Shield: Taiwan's Protection Against Chinese Attack*, (Irving, Texas: Fusion Press, 2001).

[44] The Executive Yuan develops Taiwan's counter-terrorism policy. The Ministry of Interior's National Police Agency (NPA) is responsible for counter-terrorism, senior leadership protection, and critical infrastructure protection (CIP). The NPS's Special Security Service Forces (*wei'an*) have three corps (1st, 4th, and 5th) to cover the island. The NPA's 2nd Corps handles CIP duties for facilities, including nuclear power plants, under the National Science Council and Ministry of Economic Affairs. The NPA's 3rd Corps is responsible for border control and its 6th Corps for senior leadership protection. The military also has specialized counter-terrorism units under the Military Police, Army, and Marines.

[45] *2006 National Security Report*, National Security Council, May 20, 2006. The opening ceremony for the Megaports Program was conducted in Kaohsiung in November 2009.

[46] Cecilia Fanchiang, "Taipei Burdened By Illegal Chinese Immigrants," *Taiwan Aujourd'hui*, September 26, 2003, at http://taiwanauj.nat.gov.tw/ct.asp?xItem=20258&CtNode=122, accessed on April 20, 2008. The publication is connected with the French representative office in Taipei. Responsibility for monitoring and controlling Taiwan's borders lies with the Coast Guard Administration and NPA. The Coast Guard monitors Taiwan's coastal waters, while the NPA oversees access.

[47] Shirley A. Kan, *Taiwan: Major U.S. Arms Sales Since 1990*, Congressional Research Service, December 2, 2009, at http://assets.opencrs.com/rpts/RL30957_20091202.pdf, accessed on January 12, 2010. After initial discussions in December 1999, the Bush Administration notified Congress of a proposed sale of JTIDS/Link 16 terminals in July 2001. Also see Edward W. Ross, "Improving Taiwan's Military Capabilities, C4ISR Integration," presentation before the U.S.-Taiwan Business Council defense conference, September 27-29, 2009.

[48] Among various sources, see Michael Swaine, "Deterring Conflict In The Taiwan Strait: The Successes and Failures of Taiwan's Defense Reform and Modernization Program," *Carnegie Papers,* No. 46, July 2004, at http://www.carnegieendowment.org/files/CP46.Swaine.FINAL.pdf, accessed on December 20, 2009. Also see "Po Sheng Decision Imminent," *Taiwan Defense Review*, July 17, 2003.

[49] See Kenneth Allard, *Command, Control, and the Common Defense*, (Washington DC: National Defense University, 1996), p. 211.

[50] Among various sources, see David S. Alberts, John J. Garstka, and Frederick P. Stein. *Network Centric Warfare*, (Washington DC: DoD C4ISR Cooperative Research Program, September 1999). For another outstanding overview of network centric warfare, see Clay Wilson, *Network Centric Operations: Background and Oversight Issues for Congress*, Congressional Research Service Report to Congress, March 15, 2007. In accordance with Metcalf's Law, the value" or power of a network increases in proportion to the square of the number of nodes on the network. Technology is advancing to the point to where a common operational picture could be used on a personal display assistant (PDA).

[51] JTIDS forms the backbone of a common tactical picture. Operating in the L-band, between 969 MHz and 1.206 GHz, with a data rate of 238 kilobits per second (kpbs), and possible speed of up to 2 megabits per second (mbps), JTIDS provides a secure high-speed network for communications, navigation, and identification. While frequency hopping is an effective means of countering jammers, it only uses a small portion bandwidth at any one time. Therefore, the amount of data that JTIDS carries is relatively limited to 54 kilobits per second, although some references note that the data rate could be as high as 1 megabit per second. See Dr. Carlo Kopp, "Network Centric Warfare Fundamentals," *Defence Today Magazine*, January/February 2005, and "Introduction To Tactical Digital Information Link J And Quick Reference Guide," DoD Air Land Sea Application Center, June 30, 2000.

[52] For an overview of JTIDS, see Dr. Carlo Kopp, "Network Centric Warfare Fundamentals," *Defence Today Magazine*;and Introduction to Tactical Digital Information Link J And Quick Reference Guide, DoD Air Land Sea Application Center June 30, 2000.

[53] The specific JTIDS variant is known as the Multifunctional Information Distribution System (MIDS).

[54] For an introduction to some of Taiwan's C4ISR upgrades, see Wendell Minnick, "Electronic Fortress: Taiwan's Military Grapples with a Major C4ISR Upgrade," *C4ISR Journal*, March 2, 2007, at http://www.isrjournal.com/story.php?F=2366056, accessed on September 2, 2009. The Po Sheng program was also to connect with other networks, including the Military Information and Communications System (MICS), the ROC Army's Integrated Mobile Subscriber Equipment (IMSE), the Air Force's E-2T and Qiangwang/Anyu-4 system, and the Navy's Ta-Chen system. Intelligence, surveillance, and reconnaissance (ISR) assets were not included. Interviews in Taipei, October/November 2009. Also see Edward W. Ross, "Improving Taiwan's Military Capabilities, C4ISR Integration," presentation before the U.S.-Taiwan Business Council defense conference, September 27-29, 2009.

[55] For an excellent discussion of Taiwan's C4ISR programs and requirements, see Edward W. Ross, "Improving Taiwan's Military Capabilities, C4ISR Integration," presentation delivered at the US-Taiwan Business Council Defense Conference, September 27-29, 2009.

[56] The initial Congressional notification that was submitted in July 2001 included only 50 JTIDS/MIDS terminals. However, DoD announced the sale of another 35 MIDS terminals and 25 ship-borne MIDS on January 29, 2010. See "Taiwan – Joint Tactical Information Distribution System," *DSCA News Release*, July 18, 2001, at http://www.dsca.mil/PressReleases/36-b/Taiwan%2001-19.pdf, accessed on November 2, 2009; and Taipei Economic and Cultural Representative Office in the United States, "Multifunctional Information Distribution Systems (MIDS)," *DSCA News Release*, January 29, 2010, at http://www.dsca.mil/PressReleases/36-b/2010/Taiwan_09-37.pdf, accessed on February 1, 2010.

[57] Interview, October 20, 2009. For further background on the program, see "Po Sheng Progress," *Taiwan Defense Review*, June 16, 2005.

[58] Edward W. Ross, "Improving Taiwan's Military Capabilities, C4ISR Integration," presentation before the U.S.-Taiwan Business Council defense conference, September 27-29, 2009.

[59] Although not confirmed, Taiwan media reporting asserts that at least one future communications project is known as the "AN-SHUN" program (安訊專案).

[60] See "President Ma Ying-jeou's National Day Address," *TECRO Press Release*, October 10, 2009, at http://www.roc-taiwan.org/US/ct.asp?xItem=111867&ctNode=2300&mp=12, accessed on November 23, 2009.

[61] For background on the global importance of remote sensing satellites, see United Nations Resolution 41/65, *Principles Relating to Remote Sensing of the Earth from Space*, December 3, 1986, at http://www.un.org/documents/ga/res/41/a41r065.htm, accessed on September 12, 2009; and "International Charter On Cooperation To Achieve The Coordinated Use Of Space Facilities In The Event Of Natural Or Technological Disasters," April 25, 2000, at http://www.disasterscharter.org/charter, accessed on January 10, 2010.

[62] "Satellite Prospects," *Taiwan Defense Review*, October 20, 2004.

[63] ibid. After encountering delays in the U.S. licensing process, Taiwan opted to procure Formosat-2 from France's Astrium at a contract price of around US$70 million.

[64] Albert Lin and Chien-Fang Lai, "The Command and Data Management Unit For NSPO Formosat-5 And Future Satellites," conference paper for the Fourth Asian Space Conference 2008, Taipei, Taiwan, October 1-3, 2008. Also see an overview of the Formosat-5 on the NSPO's website, at http://www.nspo.org.tw/2008e/projects/project5/intro.htm. For more recent reporting, see Bryan Chuang and Adam Hwang, "Taiwan To Develop and Make Satellite-Loaded Remote Sensing Instrument," *Digitimes*, February 3, 2010, at http://www.digitimes.com/news/a20100203PD201.html, accessed on February 10, 2010.

[65] Way-Jin Chen, Vicky Chu, J. R. Tsai, "Taiwan's First Self-Reliant Micro Satellite," conference paper for the Fourth Asian Space Conference 2008, Taipei, Taiwan, October 1-3, 2008. Also see an overview of the program on the NSPO website, at http://www.nspo.org.tw/2008e/projects/project6/intro.htm.

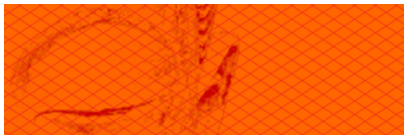
[66] Interviews in Taipei, November 2009.

[67] For background, see the Group on Global Observation website at http://www.earthobservations.org/, accessed on December 20, 2009.

[68] See "TIEOS 2009: Taiwan Integrated Earth Observation System Forum," National Applied Research Laboratory website, http://www.narl.org.tw/event/2009/tieos/index.html.

[69] NASA, "Satellites Guide Relief to Earthquake Victims," *Science@NASA*, June 19, 2009, at http://science.nasa.gov/headlines/y2009/18jun_servir.htm, accessed on November 18, 2009.

[70] One of the greatest challenges for UAVs is not necessarily in the airframe but in the bandwidth requirements. UAVs often come with a unique data link system that connects the aircraft with the ground station. Transmission of high definition video and images requires a large amount of bandwidth. The resolution of the data will also vary according to operating altitudes make a difference. Lower altitudes offer better resolution, less haze, and shorter lenses. However, lower altitudes also mean reduced fields of view and possible line-of-sight obstacles when transmitting data to ground stations. On the other hand, UAVs at



higher altitudes have less obstructed transmissions, but also lower resolution data. However, they can also serve as high altitude communications relays, thus extending the range of a communications network.

[71] Author interviews in Taipei, October 2009. Also see "Taiwan Army Still On Track for Unmanned Aerial Vehicle in 2011," *Taiwan News*, July 6, 2009.

[72] Lt Col Ed "Mel" Tomme and Col Sigfred J. "Ziggy" Dahl, "Balloons in Today's Military? An Introduction to the Near-Space Concept," *Air & Space Power Journal,* Winter 2005. Also see Lt Col Edward B. Tomme, "The Paradigm Shift to Effects-Based Space: Near-Space as a Combat Space Effects Enabler," *Airpower Research Institute Research Paper,* January 2005. For a general Chinese analysis, see Wang Shengkai, Quan Shouwen, Li Binhua, and Ma Qin, "Near Space and Near Space Flight Vehicles" (临近空间和临近空间飞行器),*CONMILIT*, (*Xiandai junshi*), 2007(7), pp. 36-39.

[73] For details, see "Air Defense Contract Awarded," *Taiwan Defense Review*, January 20, 2004. For one of the best overviews on these and other programs, see Shirley A. Kan, *Taiwan: Major U.S. Arms Sales Since 1990*, Congressional Research Service report, September 24, 2009. The U.S. $800 million program to develop, manufacture, and deploy a long range large phased array UHF early warning radar has experienced delays. When fully operational, the early warning radar should be able to detect large numbers of ballistic and airbreathing targets at extended ranges. Like its predecessor, the radar has inherent capabilities for tracking PRC satellites, as well as providing control for Taiwan's own satellites. As an early warning system, the radar is not expected to survive past initial strikes in a full scale amphibious assault. Air surveillance assets include a range of other new and existing radar systems operating in the L- and S-Band portions of the frequency spectrum.

[74] For a detailed assessment on passive radar systems, see T. Smestad, H. Øhra, and A. Knapskog, *ESM Sensors for Tactical Information in Air Defence Systems*, Norwegian Defence Research Establishment, at ftp.rta.nato.int/public//PubFulltext/RTO/MP/RTO-MP...///MP-063-09.pdf, accessed on October 20, 2009. Passive radar systems are often referred to as "multistatic" since they use three or more stationary transmitters and receivers.

[75] For a technological assessment, see Baris Calikoglu, *Evaluation And Analysis Of Array Antennas For Passive Coherent Location (PCL) Systems*, (Dayton, OH: Air Force Institute of Technology, 2002). Also see Arend G. Westra, "Radar versus Stealth: Passive Radar and the Future of U.S. Military Power," *Joint Forces Quarterly*, Iss. 55, 4th Quarter 2009. The range of IRST systems are limited in comparison to conventional radars as adverse atmospheric and weather conditions can increase the rate of attenuation.

[76] See, for example, Kao Chia Chuen, Hsu Yueh-Jiuan G., Chang Kuo-Chyang, and Chen Hwa, "The Setup of Operational Coastal Watch System," Tenth OMISAR Workshop on Ocean Models, November 1-3, 2002. The authors are from the National Chengkung University, Central Weather Bureau, and Water Resources Agency.

[77] T. M. Georges and J. A. Harlan, "The Case for Building a Current-Mapping Over-the-Horizon Radar," Proceedings of the IEEE Sixth Working Conference on Current Measurement, March 11-13, 1999, San Diego, CA, at http://ccar.colorado.edu/~harlanj/ieee_curr99.htm, accessed on October 15, 2009. The authors are from the National Oceanic and Atmospheric Administration.

[78] See, for example, "Tapping into the Navy's Listening System," *Popular Science*, October 1995, p. 28. For application in marine life conservation, see "Whale Monitoring Using the United States Navy Integrated Undersea Surveillance System (IUSS)," U.S Navy Strategic Environmental Research and Development Program, Paper CS-48, at http://www.p2pays.org/ref/22/21724.pdf.

[79] Karl Hasslinger, "Undersea Warfare: The Hidden Threat," *Armed Forces Journal*, March 10, 2008. Also see Richard Burgess, "New Tracker," Navy League announcement, May 2006, http://www.navyleague.org/sea_power/may06-24.php, accessed on November 10, 2009.

[80] Since spectrum below 300MHz is close to saturation, cell phones generally operate in the 400MHz to 2.5GHz range.

[81] Kiyoko Nagami et. al., "Satellite Communications for Supporting Medical Care in the Aftermath of Disasters," *Journal of Telemedicine and Telecare*, Vol. 12, 2006, pp. 274–275.

[82] Anshell J. Schiff and Alex K. Tang, *Chi-Chi, Taiwan, Earthquake, Lifeline Performance*, Technical Council of Lifeline Earthquake Engineering, Monograph No. 18, July 2000. The earthquake took place as the author and a team of U.S. defense specialists were in Taiwan and assessing certain aspects of Taiwan's military capabilities.

[83] See Franklin D. Kramer and John C. Cittadino, "Sweden's Use of Commercial Information Technology for Military Applications," *Defense Horizons*, No. 50, Center for Technology and Security Policy, National Defense University.

[84] *White Paper on Emergency Communications*, Prepared by the Space & Advanced Communications Research Institute (SACRI), George Washington University, January 5, 2006.

[85] A general definition of broadband is a system that is greater than 1 megabits per second. Narrowband is below 100 kilobits per second, and wideband is between 100kbps and 1mbps.

[86] "Radio Program Faces Restructure," *Taiwan Defense Review*, August 29, 2006. The original requirement submitted in 1998 was for between 10,000-14,000 units, with at least six naval and other variants. The program has been placed on hold. Designed and developed by the CSIST and introduced into the active inventory in 2009, the PRC-37A combat network radio system operates in the 30-88 MHz band and is expected to have a range of approximately 50-kilometers.

[87] See "Networking HF," *Taiwan Defense Review*, November 11, 2005; and "High Frequency Radio System Public Announcement," Procurement Center - Ministry of National Defense, May 2006. Original planning involved the procurement of almost 1000 HF radios for both military and civilian use. . With requirements for encryption, the radio operates on 280,000 channels between 2-30 MHz, and should be interoperable with Link 11 (HF and UHF frequency system used by U.S. Navy) and IP-based communication systems. A key characteristic would be automated link exchange (ALE), which automatically selects a frequency to link to stations in a network without operator assistance. The program had been valued at as much as US$142.8 million (NT $4.6 billion).

[88] As an early adaptor of the technology, Taiwan's WiMAX network uses different sets of frequencies, including 2.5-2.69 and 3.4-3.7 GHz for broadband wireless access. It also uses 608-680 MHz and 686-710 MHz for high definition TV. Adhering to IEEE 802.16e standards, Taiwan was has been granted licenses for manufacturing of WiMAX chipsets and companies are manufacturing specialized base stations. Initial services were scheduled for Penghu in April 2009, and for Kaohsiung in Summer 2009.

[89] WiMAX IEEE-802.16 Military Applications, *Defense Update*, Iss. 3, 2005. For an overview of Taiwan's WiMAX program, see *The M-Taiwan Program: Paving the Way for WiMAX Ecosystem*, briefing by the Ministry of Economic Affairs Industrial Development Bureau, October 23, 2007. Eventually, Taiwan's WiFi and cell phone networks are likely to merge with WiMAX. While WiMAX offers impressive capabilities, it remains vulnerable to jamming. Regulatory restrictions and a desire to minimize interference with other communications networks have resulted in a vulnerable signal that is susceptible to intrusion in a crisis. However, the evaluations of a commercial technology for military applications should not be based strictly on its known vulnerabilities, as they can be addressed through modest redesign.

[90] See "M-Tube UMPC with VIA Processor Supports WiMAX," *My Digital Life*, October 11, 2007, at http://www.mydigitallife.info/2007/10/11/m-tube-umpc-with-via-processor-supports-wimax, accessed on December 1, 2009.

[91] Among various sources, see JTRS Factsheet, U.S. Department of Defense Joint Program Executive Office for the Joint Tactical Radio System, September 2009, at http://jpeojtrs.mil/files/domains/JTRS_media_Updated_Sept09_final.pdf, accessed on November 15, 2009; and "The Market for Multimission Communications Systems," *Forecast International*, August 2007.

[92] "UMC Delivers Leading-edge 65nm FPGAs to Xilinx," http://www.dsp-fpga.com/news/db/?4512, accessed on October 29, 2009; "General Dynamics Selects Xilinx FPGA for JTRS Multifunction Radios," *Military & Aerospace Electronics*, May 1, 2006; Jack Browne, "Tracking Trends In Military-Electronics Technologies," *Microwaves and RF*, September 2007, at http://www.mwrf.com/Articles/Index.cfm?ArticleID=16646&pg=2, accessed on October 10, 2009; Jeff Child, "FPGA Tech Advances Propel Software Radio Forward," *COTS*

Journal Online, October 2006, at http://www.cotsjournalonline.com/articles/view/100566, accessed on November 2, 2009.

[93] Dean Collins, "Trust But Verify," DARPATech Symposium, August 7, 2007, Anaheim, California. Dean Collins has been Deputy Director, DARPA Microsystems Technology Office. Taiwan's UMC manufactures Xilinx Virtex 4, Virtex 5, Virtex 6, and Spartan 6 FPGAs. The latter two are 40 and 45nm respectively. TSMC manufactures Altera Stratix IV FGPAs, the first sub-65nm devices on the world market. Stratix IV FPGAs, are based on TSMC 40-nm process technology, and touted as surpassing "all other high-end FPGAs, with the highest logic density, most transceivers, and lowest power requirements." Among various sources, see "General Dynamics selects Xilinx FPGA for JTRS Multifunction Radios," *Military and Aerospace Electronics*, May 2006, at http://mae.pennnet.com/display_article/255394/32/ARTCL/none/none/1/General-Dynamics-selects-Xilinx-FPGA-for-JTRS-multifunction-radios/. Also see "Stratix IV Device Family Overview," Altera website, at http://www.altera.com/literature/hb/stratix-iv/stx4_siv51001.pdf.

[94] See *Report of the Defense Science Board Task Force On High Performance Microchip Supply*, Defense Science Board, February 2005. Sally Adee, "The Hunt for the Kill Switch," *IEEE Spectrum*, May 2008, at http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0, accessed on November 10, 2009.

[95] For example, see National Technology Plan for Networked Communications: Key Research and Administrative Guidance [網路通訊國家型科技計畫: 研究重點規劃及執行簡要], October 2009, ROC National Science Council. Yao-Nan Lien, Li-Cheng Chi, and Yuh-Sheng Shaw, "A Walkie-Talkie-Like Emergency Communication System for Catastrophic Natural Disasters," paper presented at the International Symposium on Pervasive Systems, Algorithms, and Networks (I-SPAN), Kaoshiung, December 14-16, 2009, at http://www.cs.nccu.edu.tw/~lien/Pub/c79u1net.pdf , accessed on January 2010; and Yao-Nan Lien, Hung-Chin Jang and Tzu-Chieh Tsai, "A MANET Based Emergency Communication and Information System for Catastrophic Natural Disasters," Proceedings of the IEEE Second International Workshop on Specialized Ad Hoc Networks and Systems, June 26, 2009. The authors are from the Computer Science Department at Cheng-chi University. Also see Brent A. Peacock, "Connecting The Edge: Mobile Ad-Hoc Networks (MANETs) for Network Centric Warfare," *Blue Horizons Paper*, Center for Strategy and Technology, U.S. Air Force War College, April 2007.

[96] For one of the best overviews of cognitive radio trends, see Kwang-Cheng Chen and Ramjee Prasad, *Cognitive Radio Networks*, (West Sussex: Wiley, 2009). Chen is from Taiwan University. Also see Steven Ashley, "Cognitive Radio," *Scientific American*, February 20, 2006. Also see John S. Powell, "Cognitive and Software Radio: A Public Safety Regulatory Perspective," unpublished paper for the National Public Safety Telecommunications Council (NPSTC) Software Defined Radio Working Group. Also Simon Haykin, Cognitive Radio: Brain-Empowered Wireless Communications, *IEEE Journal On Selected Areas In Communications*, Vol. 23, No. 2, February 2005.

[97] See Chuang Yu-Min, "UWB Roadmap of CSIST: A Faithful Partner of the Taiwan UWB Industries," briefing, April 12, 2006; and James W. McCulloch and Bob Walters, "Military Applications Of Ultra-Wideband Communications," *Journal Of Battlefield Technology*, Vol. 8, No. 3, November 2005, p. 211.

[98] "New Fiber Optic Backbone Network," *Taipei Times*, February 9, 2004, p. 4.

[99] Seymour Shapiro, James G, Murray, Robert F Gleason, Stuart R Barnes, Brian A Eales, and Paul R Woodward, "Threats to Submarine Cables," paper presented at SubOptic'97, San Francisco.

[100] F. W. Lacroix, Robert W. Button, John R. Wise, Stuart E. Johnson, *A Concept of Operations for a New Deep-Diving Submarine*, RAND, 2001, pp. 141-143. Taiwan's existing cables include GPT, Hon-Tai, APC 2–3, APCN, and SEA-ME-WE-3. New or planned cable lines include China-U.S. 4, APCN2 (connecting Taiwan and Hong Kong), and H-P-T. The impairment to communications from undersea cable ruptures are partially mitigated by redirecting traffic via satellite. However, Taiwan's current satellite links are limited and its satellite earth stations (especially at Yangmingshan and Fangshan) are also vulnerable in an armed conflict. The final backup system would be mobile satellite services, such as Thuraya, Telstra, and Iridium; and/or Skystar services associated with Israel's Gilat satellite network. However, all satellite communications are subject to interference from ground-based jammers placed either in the footprint of these satellites or off the coast of Taiwan.

[101] "Subsea Landslide is Likely Cause of SE Asian Communications Failure," International Cable Protection Committee Ltd (ICPC) Press Release, March 21, 2007, at http://www.iscpc.org/information/ICPC_Press_Release_Hengchun_Earthquake.pdf, accessed on September 10, 2009.

[102] Dan Nystedt, "Typhoon Morakot Severs Three Undersea Internet Cables," *IDG News Service*, August 12, 2009.

[103] "Mobile Satellite Base Stations To Aid Relief Work," *Commercial Times*, September 1, 2009, at http://www.taiwantoday.tw/ct.asp?xitem=61990&ctnode=413&mp=9, accessed on September 10, 2009.

[104] "Taiwan, Singapore to Cooperate Again on Commercial Satellite," *Central News Agency*, September 19, 2008.

[105] Wu Cenxi, "Satellite Interruption Leads Taiwan to Investigate," *Epoch Times*, October 10, 2009.

[106] K.C. Jones, "Anti-Jamming Technology Offered To Commercial Satellite Firms," *Information Week*, April 9, 2007.

[107] See John Borland, "Japan Launches Extra-High-Speed Broadband Satellite," *Wired*, February 25, 2008. A communications satellite need not be useful only during a disaster. For example, Japan's Kizuna offers its entire territory high speed internet, which is particularly useful for mountainous regions and remote islands are not well-equipped with Internet infrastructure due to its costs. The KIZUNA (WINDS) does not require costly ground equipment. If one installs a small antenna (about 45 cm or about 17 inches in diameter) at your house, data can be received at up to 155Mbps and transmitted at up to 6 Mbps. With a larger antenna of about 5 meters in diameter, super high-speed data communications of up to 1.2 Gbps will be available. Another model could be Thailand's IPStar broadband communications satellite, which was launched in late 2005. Like KIZUNA, IPStar offers broadband internet to users in the region, as well as voice and datacasting services. Another satellite, owned by New Skies Satellites, operates a system with twelve super-high-gain uplink spot beams, each approximate 650 kilometer in diameter, in the K_a-band that cross over to K_u-band downlink beams and also offers IP-based services.

[108] Mobile satellite services today include systems such as Thuraya, Telstra, and Iridium; and/or Skystar services associated with Israel's Gilat satellite network. Inmarsat, an international company, operates a constellation of 11 geostationary satellites with global, wide spot, and narrow spot beams. The latter will be the backbone of Inmarsat's planned Broadband Global Area Network (BGAN) services. BGAN, also known as SwiftBroadband, will offer up to 492 kbps, which can be used to support Internet services and GSM. When the system is complete there will be three satellites, one positioned over each major ocean (Pacific, Atlantic, and Indian).

[109] When a terrestrial infrastructure – whether wired or wireless – fails, internet access and other data links can be sustained. This would include the ability to transmit images, streaming video, and other forms of information requiring large bandwidth and high speed. Specialized amplifiers could adjust signal power as needed to compensate for rain attenuation. A broadband communications satellite can ensure "remote medicine" that enables everybody to receive sophisticated medical treatment regardless of time and location by transmitting clear images of the conditions of a patient to a doctor in an urban area from a remote area or island where few doctors are available. In academic and educational fields, schools and researchers in remote areas can exchange information easily.

[110] See *Coalition Warrior Interoperability Demonstration 2005 Final Report: Mobile Enhanced Situational Awareness Network* (MESA; IT02.62), undated, at http://www.cwid.js.mil/public/htmlfiles/262int.html#tech, accessed on October 2, 2009.

[111] At least four satellite radio services are operating in the global market today. Within the Asia-Pacific region, MBSAT provides multi-channel video, audio and data casting services for mobile users throughout Japan and Korea. Owned by Mobile Broadcasting Corporation (MBCO), SK Telecom, Toyota, and 74 other companies, the satellite was in March 2003 from Cape Canaveral and provides satellite digital audio broadcasting to subscribers throughout Japan. Using MBCO's Loral-built satellite that operates in the S-Band (2.5 GHz), Japan began trials of its satellite radio system for disaster warning, recovery, and response in 2006.

[112] Xu Hong, "Taijun dasuan taiwanban dixia 'Wujiao dasha' " [Taiwan's military plans to establish underground 'Pentagon'], *Quanqiu shibao* [World news], September 15, 2000. Also see Lou Chao-lung, "The Hengshan Command Post: A Key Position From Which To Defeat The Enemy," *Chung-kuo shihpao*,September 8, 2000 (FBIS: FTS19990923001655); and Brian Hsu, "Air Force Shows Off Command Centers," *Taipei Times*, September 8, 2000. According to *Jane's Defense Weekly*, the Qiangwang, or Strong Net air defense network, includes four Control and Reporting Centers, and is controlled by the Taiwan Air Force's Kungkuan Anti-Aircraft Operations Center in Taipei. The Qiangwang system will be supplemented by a long range UHF early warning radar system. See Wendell Minnick, "Taiwan Targets $30 Million for Radar Upgrades," *Jane's Defense Weekly*, November 6, 2000. The Hengshan system includes the Navy's Dacheng sub-system, the Air Force's Qiangwang sub-system, and the Army's Lu'zi sub-system. Under the Brotherhood Project, initiated in 1993, there are allegedly plans to establish a Dazhi Strategic District that will house the Ministry of National Defense and a staff of 5000-6000 individuals in the vicinity of the Hengshan Command Center.

[113] Lin Li-Wei and Wang Tzong-Luen, "Evaluation in Design of Taipei City Emergency Operations Center," at http://www.disaster.org.tw/chinese/annmed/vol2no2/3.pdf.

[114] At lower echelons, county and city governments with disaster management units form their own command center to coordinate emergency responses. The CEOC, however, remains the central coordinator and serves to communicate significant disaster information to the local command centers in order to achieve minimal loss from, and rapid response to, the disaster.

[115] See *Annual Report of the Center for Disease Control*, published in June 2006. According to its website, the CDC and NHCC are located in Taipei that incorporate elements of the U.S. Incident Command System and the SARS Command System SOP.

[116] See "Disaster Response Bill Proposed," *Taipei Times*, December 28, 2009, p. 3, at http://www.taipeitimes.com/News/taiwan/archives/2009/12/28/2003462025, accessed on January 6, 2010; and interviews in Taipei, January 2010.

[117] For details, see "Air Defense Contract Awarded," *Taiwan Defense Review*, January 20, 2004.

[118] For a detailed assessment of MDA, see John C Rienzo, "Net Centric Domain Awareness: Automated Ways To Create Knowledge From Chaos," conference paper presented at *Maritime Trade And Security: Striking The Right Balance*, January 11-12, 2007, Mumbai, India.

[119] Ostensibly due to funding shortfalls, the command and control portion of the Po Sheng program is said to be related to a prototype U.S. Coast Guard Harbor and Coastal Security system, also known as Hawkeye. Hawkeye was sponsored by the U.S. Department of Homeland Security Office of Science and Technology as a prototype development effort. Originally intended to link radars, cameras, Automatic Identification System (AIS), and other sensors to a central command center, the commercial system is said to have limitations in terms of data fusion capacity and user friendliness. As a result, further improvements in Taiwan's strategic and operational-level command and control system may be appropriate. See Robert K. Ackerman, "Harbor Security Melds Sensors, Databases," *Signal Magazine*, February 2008. Automatic Identification System (AIS) provides basic shipping information, mandated by the International Maritime Organization for ships more than 300 gross tons and all passenger ships.

[120] For background, see *National Plan To Achieve Maritime Domain Awareness For The National Strategy For Maritime Security*, Department of Homeland Security, October 2005, at http://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf, accessed on November 10, 2009.

[121] It is worth noting that close to one-half of the world's ocean transport involves the movement of petroleum products.

[122] Andrzej Jeziorski, "Toward Transformation: Singapore Focuses on ISR Purchases," *C4ISR Journal*, January 4, 2008.

[123] See Franklin D. Kramer and John C. Cittadino, "Sweden's Use of Commercial Information Technology for Military Applications," *Defense Horizons*, No. 50, Center for Technology and Security Policy, National Defense University.