



NPS IN THE NEWS

Weekly Media Report – Aug 23 - 29, 2022

Further reproduction or distribution is subject to original copyright restrictions.

SECNAV:

[SECNAV Visits FNMOC](#)

(Navy.mil 22 Aug 22) ... Lt. Lauren Dulle

Secretary of the Navy (SECNAV) Carlos Del Toro visited Fleet Numerical Meteorology and Oceanography Command (FNMOC) in Monterey, California, August 18... Del Toro is visiting San Diego and Monterey to visit with Sailors and Marines at installation commands, engage with leadership at the Surface Warfare Flag Officer Training Symposium, and to discuss strategic initiatives at the **Naval Postgraduate School**.

RESEARCH:

[AT&T Partners With Military for Maritime 5G, Edge Compute Experiments](#)

(Fierce Wireless 16 SEPT 21) ... Bevin Fletcher

AT&T has a new agreement with the U.S. military that includes experiments to connect unmanned robots, aerial drones and autonomous underwater vehicles in a single system, assisted by 5G and edge computing... It's a three-year collaborative research and development agreement with the **Naval Postgraduate School** (NPS) to support a variety of 5G-focused experiments at NPS facilities. NPS is the Department of the Navy's applied research university.

[Experts to Gather in Helsinki to Examine Littoral Operations in Baltic Sea](#)

(Marine Link 22 Aug 22) ... Edward Lundquist

(Sea Power 22 Aug 22) ... Edward Lundquist

Naval and maritime experts will be convening in Helsinki, Finland, for the Littoral OpTech Baltic Sea workshop. The event will take place August 30 and 31 at the Finnish Naval Academy... The Helsinki symposium is the latest in the series of OpTech workshops, which have been held since 2014 in Stockholm, Sweden; Tokyo, Japan; Cartagena, Columbia; Halifax, Canada; and Souda Bay, Greece; with additional meetings held at the U.S. **Naval Postgraduate School** in Monterey, Calif.

[The State of the Warfighter Mentality in the SWO Community](#)

(CIMSEC 25 Aug 22)

(Real Clear Defense 25 Aug 22)

As the United States shifts focus from the Global War on Terror to peer competitors, senior naval leaders have increased messaging to the fleet that focuses on preparing for war at sea. Considering this shift, I investigated the state of the warfighter mentality in the Surface Warfare Officer (SWO) community to gauge how the community felt about its own readiness as part of my program at the **Naval Postgraduate School**. Although the Navy gauges readiness in many ways, my goal was to go directly to the source by interviewing members of the SWO community – while avoiding the constraints and endemic fatigue so common in survey methodology. I used semi-structured interviews to identify attitudes, opinions, and trends related to the warfighter mentality across the ranks of O-2 to O-6. I conducted 23 interviews with volunteer subjects, each lasting one to three hours. Participants in this research study came from different commands and their tactical and operational experiences varied widely.



STUDENTS:

[SOF and Field Sanitation: The Importance of a Healthy Partner Force](#)

(Small Wars Journal 30 Aug 22) ... Maj. Pete Reider

The development and implementation of effective field sanitation and hygiene procedures marked a revolutionary step in battlefield technology. It marked a critical turning point in the early 20th century when the number of soldiers killed from disease or infection was proportionately less than those who died in or were wounded through combat. US planners began to address this problem following the First World War and it was at this point the US transitioned, as Vincent Cirillo notes, from the disease era to the trauma era... MAJ Pete Reider is a active duty Civil Affairs Officer, with multiple deployments to the CENTCOM AOR. He is currently a graduate student at the **Naval Postgraduate School** studying defense analysis.

FACULTY:

[Uncertain Outcomes Will Likely Result From China's Military Display Over Taiwan](#)

(English News Track 23 Aug 22) ... Aniket Dixit

China: The world's largest standing army was able to test the coordination of its personnel, weapons, supplies, and communications thanks to China's massive intimidation campaign this month in response to US House Speaker Nancy Pelosi's trip to Taiwan, although the results are not entirely clear, analysts said in Washington on Monday... However, the US navy will want to avoid coming off as complacent or appearing to accept Chinese military vessels entering Taiwanese waters after crossing the median line. That could then start a potential escalation cycle of tit-for-tat. Christopher Twomey, an associate professor at the US **Naval Postgraduate School**, stated that "this is most likely the early stages of a crisis that is going to continue to percolate for months."

[As China's Navy Grows Ever Larger, So Does the Threat to Taiwan](#)

(Japan Times 25 Aug 22) ... Gabriel Dominguez

(Transcontinental Times 25 Aug 22) ... Gabriel Dominguez

As Beijing ramps up military activities around Taiwan, the steady growth and modernization of China's naval fleet is fueling concerns about how Beijing could use what is already the world's largest navy in a move against the self-ruled island... This destroyer class "is the culmination of substantial experimentation in ship design by the PLA Navy over the preceding decades. With the 052D, the Chinese have finally found a design they are satisfied with, and they have been engaging in serial production in recent years, with over 14 currently in the fleet," said Christopher Twomey, assistant professor of national security affairs at the U.S. **Naval Postgraduate School** in Monterey, California, emphasizing that he was not speaking on behalf of the U.S. Navy.

[Restraining Russian Ransomware](#)

(FPRI 25 Aug 22) ... Scott Jasper

Last May, Americans up and down the East Coast waited in long lines for gas. The panic wasn't caused by a foreign war or sanctions—it was triggered by a Russian ransomware attack. The Russia-based criminal group DarkSide had infected Colonial Pipeline with ransomware and demanded millions of dollars to unlock Information Technology systems. Colonial shut down the flow of fuel from the Gulf Coast for a week, even after paying the hackers roughly \$5 million... Scott Jasper is a senior lecturer at the **Naval Postgraduate School** in Monterey, California, and the author of "Russian Cyber Operations: Coding the Boundaries of Conflict" by Georgetown University Press.

[The Fourth Taiwan Strait Crisis is Just Starting](#)

(War on the Rocks 22 Aug 22) ... NPS Christopher P. Twomey

The Chinese military exercises that began on Aug. 3, 2022, have initiated the Fourth Taiwan Strait Crisis. The most immediate reason for this was Speaker Nancy Pelosi's visit to Taipei. But this is a bigger crisis, driven by bigger factors. There has been a steady erosion in Sino-American relations and — not unrelated — a shift in the nature of U.S.-Taiwan relations that Beijing finds deeply threatening. As a result, expectations of a rapid resolution to the crisis are chimeric, as too are blithe expectations of a quick return to the status quo ante.



[How is China Trying to Redefine Power Balance in Taiwan Strait?](#)

(DW 25 Aug 22)

Beijing's pledge to conduct "regular patrols" near Taiwan after large-scale military drills points to a worrisome and dangerous development, according to analysts... The ratcheting up of tensions between China and the US, and Beijing's pledge to conduct "regular patrols" near Taiwan, point to a worrisome and dangerous development, said Christopher Twomey, an expert on security affairs at the US **Naval Postgraduate School** in California.

ALUMNI:

[Salona Global Expands Management Team to Scale for Growth; Appoints New Chief Financial Officer for Salona, President for SDP Unit; Executes National Sales Distribution Agreement with Digitsole](#)

(Globe Newswire 22 Aug 22)

Salona Global Medical Device Corporation ("Salona Global," "SGMD," or the "Company") (TSXV:SGMD) announced that, in line with its rapid growth, it has appointed an experienced public company executive as Chief Financial Officer ("CFO") and promoted an operational executive as President of South Dakota Partners, Inc. ("SDP"), one of the Company's operating subsidiaries. Additionally, the Company has executed a national sales distribution agreement with Digitsole U.S Inc. ("Digitsole")...Effective today, Mike Plunkett has been promoted to President of SDP, to replace Luke Faulstick, who was appointed CEO of Salona Global on July 18, 2022. Mr. Plunkett has served as a general manager for SDP since January 2019. Prior to that, Mr. Plunkett spent 25 years in the U.S. Navy rising to rank of Captain before moving into the private sector in multiple senior leadership roles including President of Alphatec Spine, Inc. Mr. Plunkett received a B.S. in Accounting from Saint John Fisher College, an M.S. in Financial Management from the **Naval Postgraduate School**, and an M.A. from the Naval War College.

[Wisconsin Deputy Adjutant General For Air Completes Executive Leaders Program at Naval Postgraduate School](#)

(Wisconsin National Guard 23 Aug 22) ... Sgt. 1st Class Katie Theusch

(Wisconsin Politics 23 Aug 22) ... Sgt. 1st Class Katie Theusch

Brig. Gen. David May, the Wisconsin National Guard's deputy adjutant general for Air, completed the Executive Leaders program at the Naval Postgraduate School Center for Homeland Defense and Security (CHDS) on August 11th.

[USMSM Gets New Board Chair; Keane to Serve for Three Years](#)

(Southern Maryland News 23 Aug 22) ... Caleb M. Soptelean

Jack Keane was recently named board chair of the University System of Maryland at Southern Maryland in California...In 1993, he graduated from the **Naval Postgraduate School** in Monterey, Calif., with a degree in operations research. He retired in 1995 at the rank of lieutenant commander after serving at the Naval Research Laboratory, where he flew research missions worldwide. Since his military career, Keane has been heavily involved in research and education.

UPCOMING NEWS & EVENTS:

Aug 30- Sept 1: [Emerging Technology Awareness \(ETA\) for the Warfighter](#)

Sept 5: Labor Day (Federal Holiday)

Sept 12-13: [Blockchain and Beyond: National Security Symposium](#)

Sept 23: [Summer Quarter Graduation](#)



SECNAV:

SECNAV Visits FNMOC

(Navy.mil 22 Aug 22) ... Lt. Lauren Dulle

Secretary of the Navy (SECNAV) Carlos Del Toro visited Fleet Numerical Meteorology and Oceanography Command (FNMOC) in Monterey, California, August 18.

Del Toro met with Sailor and Civilians, toured command facilities and received updates on FNMOC's high performance computing (HPC) upgrades, power upgrades investment, and advances in numerical modeling.

"Naval Oceanography is at the forefront of using oceanographic and meteorological data to maintain a strategic advantage," Del Toro said. "This team's enduring perseverance to deliver top tier support and continued high computing enhancements ensure mission accomplishment and the safety of our Sailors and Marines."

During the visit to FNMOC's HPC center, Del Toro received an overview of FNMOC's 24/7 operation of global and regional atmospheric and ocean models and their warfighting applications across the continuum of conflict from climate support for planning, to tactical application of oceanographic information in undersea warfare.

FNMOC, a subordinate command of Commander, Naval Meteorology and Oceanography Command, operates one of the largest single supercomputing facilities in the DoD, dedicated to environmental prediction.

"We are honored to have SECNAV visiting us today, and we are so proud to share a little bit about our mission, and our 24/7 support that ensures the safety and effectiveness of the Fleet," said CAPT Christi Montgomery, Commanding Officer of FNMOC. "Our team works tirelessly to provide on-demand environmental battlespace awareness when and where the Fleet is operating."

Del Toro is visiting San Diego and Monterey to visit with Sailors and Marines at installation commands, engage with leadership at the Surface Warfare Flag Officer Training Symposium, and to discuss strategic initiatives at the **Naval Postgraduate School**.

This visit marked SECNAV's first trip to a subordinate unit of Naval Meteorology and Oceanography Command, the Department of Defense's authoritative source for battlespace characterization from the bottom of the seafloor to the stars, generating decision advantage below, on and above the sea.

Fleet Numerical Meteorology and Oceanography Command consists of a ready Force of well-qualified, STEM-educated and scientifically trained Sailors, civilians and contractors serving in a wide-range of technical, scientific and service support billets in Monterey, California and Stennis Space Center, Mississippi.

U.S. Naval Meteorology and Oceanography Command directs and oversees more than 2,500 globally-distributed military and civilian personnel who collect, process and exploit environmental information to assist Fleet and Joint Commanders in all warfare areas to make better decisions, based on assured environmental information, faster than the adversary.

[SECNAV visits FNMOC > United States Navy > News-Stories](#)

[Return to Index](#)

RESEARCH:

AT&T Partners With Military for Maritime 5G, Edge Compute Experiments

(Fierce Wireless 16 SEPT 21) ... Bevin Fletcher

AT&T has a new agreement with the U.S. military that includes experiments to connect unmanned robots, aerial drones and autonomous underwater vehicles in a single system, assisted by 5G and edge computing.



It's a three-year collaborative research and development agreement with the **Naval Postgraduate School (NPS)** to support a variety of 5G-focused experiments at NPS facilities. NPS is the Department of the Navy's applied research university.

The main aim of the agreement is maritime technology solutions for national defense and homeland security, but could also benefit commercial industries like shipping, oil and gas, and recreational boating.

Research is slated to take place at Camp Roberts in South Monterey County, and to a lesser degree on the NPS main campus and at a beach lab north of Monterey, California. Part of the agreement involves NPS' Sea Land Air Military Research (SLAMR) program, with tests happening in the SLAMR's multi-domain laboratory.

Experiments and research will utilize millimeter wave spectrum in the 39 GHz band and mid-band LTE, according to an AT&T spokesperson.

"5G and multi-access edge computing capabilities are increasingly important in our personal lives and even more important to our warfighters," said Mike Galbraith, Department of the Navy chief digital & innovation officer, in a statement. "The collaboration between the Naval Postgraduate School and AT&T will help us explore better, faster means of collecting, disseminating, and analyzing data at the tactical edge, which is vital to maintaining and exploiting battlespace awareness."

AT&T said it's already setting up 5G network infrastructure at NPS, including a tower and short-range antenna on a pre-fabricated pad that will live at the SLAMR beach lab. The first 5G and multi-access edge compute (MEC) nodes will be installed and ready to use during the first quarter of 2022.

MEC servers will be located in an NPS datacenter and NPS will determine who or what devices can utilize the MEC services and features, according to an AT&T spokesperson. So the MEC service is private to NPS, but it's not a fully private 5G network specific to the facility.

"The functionality of MEC allows the Navy to determine what of their traffic stays locally, within their NPS facility or the beach area," the spokesperson noted, adding that the MEC does have certain mechanisms to limit the ability of other users to access the antennas.

Low latency via locally processed edge compute is expected to help speed research computing tasks.

AT&T and NPS anticipate identifying advanced technology solutions like "a connected system of unmanned and autonomous vehicles that can improve critical elements of national defense, such as multi-domain situational awareness, command and control, training, logistics, predictive maintenance and data analytics."

Research trials also will incorporate AI, robotics, IoT, machine learning, data analytics and smart base solutions.

Eventually the SLAMR program wants to have a facility for command and aquatics operations that can perform localized unmanned aerial, surface, and underwater robotic vehicle applications. AT&T said the facility, as well as some experimental vehicles, are expected to be connected via 5G and edge compute services from the carrier.

Student-led research projects are also part of the joint effort. For example, NPS Master's Degree students plan to research using VR and AR to support combat medical care for situations where a medical evacuation isn't doable. Another project focuses on 5G-powered autonomous systems in the water, specifically in the littoral zone (which is the part of sea, lake or river that is close to the shore).

"Innovation occurs at the seams and intersections of practice and expertise and NPS provides an innovation hub where this applied 5G research can occur," said Retired Vice Admiral Ann E. Rondeau, President, Naval Postgraduate School, in a statement. "AT&T's experience with the existing 5G infrastructure on the Monterey Peninsula will facilitate our collaboration on the next generation of mobile networks."

[AT&T partners with military for maritime 5G, edge compute experiments | Fierce Wireless](#)

[Return to Index](#)



Experts to Gather in Helsinki to Examine Littoral Operations in Baltic Sea

(Marine Link 22 Aug 22) ... Edward Lundquist

(Sea Power 22 Aug 22) ... Edward Lundquist

Naval and maritime experts will be convening in Helsinki, Finland, for the Littoral OpTech Baltic Sea workshop. The event will take place August 30 and 31 at the Finnish Naval Academy.

The conference will examine the integration of multi-domain operations – to include air, land, surface, undersea, space and cyber—in the crowded and cluttered coastal waters and adjacent land, and will investigate the technology and operational concepts to successfully deal with conventional, irregular and criminal threats.

The Baltic Sea has been referred to as an “extreme littoral environment” because of the varied topography (including thousands of islands), currents, varying depths and bottom types, changing temperatures and salinity, busy traffic, numerous unexploded mines and other ordnance, and undersea infrastructure such as pipelines and communications cables.

The Helsinki symposium is the latest in the series of OpTech workshops, which have been held since 2014 in Stockholm, Sweden; Tokyo, Japan; Cartagena, Columbia; Halifax, Canada; and Souda Bay, Greece; with additional meetings held at the U.S. **Naval Postgraduate School** in Monterey, Calif.

With the recent announcement about Finland and Sweden joining the NATO alliance, and concern about Russian aggression, the timing is fortuitous. However, this event was originally scheduled for two years ago, and had to be postponed due to the global pandemic.

[Experts To Gather In Helsinki To Examine Littoral \(marinelink.com\)](https://marinelink.com)

[‘OpTech’ Workshop Will Focus on Littoral Environment in Baltic Sea - Seapower \(seapowermagazine.org\)](https://seapowermagazine.org)

[Return to Index](#)

The State of the Warfighter Mentality in the SWO Community

(CIMSEC 25 Aug 22)

(Real Clear Defense 25 Aug 22)

As the United States shifts focus from the Global War on Terror to peer competitors, senior naval leaders have increased messaging to the fleet that focuses on preparing for war at sea. Considering this shift, I investigated the state of the warfighter mentality in the Surface Warfare Officer (SWO) community to gauge how the community felt about its own readiness as part of my program at the **Naval Postgraduate School**. Although the Navy gauges readiness in many ways, my goal was to go directly to the source by interviewing members of the SWO community – while avoiding the constraints and endemic fatigue so common in survey methodology. I used semi-structured interviews to identify attitudes, opinions, and trends related to the warfighter mentality across the ranks of O-2 to O-6. I conducted 23 interviews with volunteer subjects, each lasting one to three hours. Participants in this research study came from different commands and their tactical and operational experiences varied widely.

Given the current maritime stakes, understanding the fleet’s mental, tactical, and realistic state of readiness, and identifying the strengths and weaknesses in how we are preparing our warfighters is of utmost importance and was expressed passionately in every single interview conducted. Seven common themes about the warfighter mentality emerged from these interviews.

What Does the Term “Warfighter” Mean?

The survey participants shared a common framework and understanding of the characteristics of an ideal “warfighter.” Traits such as “tactical proficiency,” “sound and timely decision making,” “calm under pressure,” “physically and mentally fit,” “confident,” “competent,” and “leader” were all used to describe and define a good warfighter. However, my research suggests that the culture of the SWO community works against developing these characteristics more than it develops them. The approach to developing the warfighter mentality in the community was described as overly passive, with little to no direct or active efforts outside of entry-level indoctrination and training. As a result, rather than focusing



on warfighter development, interviewees described how a “workaholic” mentality that was prioritized instead. Officers who are afraid to fail or make mistakes, micromanage, are erosively competitive, perpetuate the “zero-defect” mentality, and/or play wardroom politics were identified as the major hinderances to community warfighter development.

Another important indicator of the state of the warfighter mentality is the level of trust that SWOs have for one another. My research suggests that there is much more distrust and cynicism in the lower ranking officers than among senior officers. The majority of junior officers (O-2 to O-4) said that they, if given the option, would only follow about 5-10% of all the SWOs they knew into combat with no reservations. Several of them could only think of one or two officers total, who they would follow without reservation. Trust improved significantly with seniority, especially at the O-6 level, where the majority said that they would follow 60–90% of all the SWOs they knew.

On the other hand, the level of dedication SWOs have to their work was identified as a positive aspect of the community and seen to bolster warfighter development. As one SWO put it, “there is a lot of goodness on the waterfront.” SWOs are dedicated to their work and want to ensure that their ships and sailors succeed. Homing in, exploiting the best parts of the community, and shifting focus to operational readiness, as the system was intended, can create confident, competent, and able crews to deploy and achieve mission success in combat. “SWOs are driven, they are proven, they understand endurance, perseverance. They are multitaskers, they can prioritize. They are leaders.” One O-6 believed that “SWOs are the hardest on SWOs. We are very hard on ourselves. There are a lot of great people in the community. If we took the time to recognize the good work that we do, we’d be a lot better off.”

Difference in Perception of Fleet Ability

My research revealed a positive link between rank and optimism regarding the Navy’s readiness to fight and win a war at sea. Senior officers in the grades of O-5 and O-6 were more optimistic about the fleet’s readiness and had more confidence that their ships, shipmates, and selves would endure combat and be successful. Conversely, junior officers had little faith in the same. At the junior levels, most admitted to not seriously thinking about preparing for a kinetic fight. For example, they reasoned that “the surface fleet had not seen real combat in a very long time,” while others were more worried about the day-to-day functions of their jobs that were unrelated to preparing for the realities of combat. However, several officers displayed a conscious and active interest in developing their warfighter mentality, warrior toughness, capabilities, or edge, attributing it to be a product of an internal drive.

It is important to note that the strongest of these convictions came from SWOs who were originally interested in serving in a different community (particularly the Naval Special Warfare community), had seen or experienced life-threatening situations, or were O-5s. In general, however, SWOs do not believe that the fleet is ready for a kinetic fight at sea. Most believed that, in the event of kinetic action, it would be an occasion to rise to; with some stepping up and leading the charge, some needing leadership and direction, and some being rendered completely useless. “The exception [wouldn’t] be those who are extremely willing, able, and capable. The exception [would] be those who aren’t.” Much of this stemmed from the way SWOs feel they are preparing themselves and being prepared by “Big Navy.” One O-6 stated that “at the O-5/O-6 level, SWOs are working hard to ready their ships and crews for battle. However, we are working under a structure that is not supportive of the end goal.” Most interviewees did not believe they were trained for the realities of combat, whether in tactics, guile, versatile skills, or bloodshed. It should also be noted that very few SWOs have ever seen combat, and even fewer have seen combat at sea.

Every SWO interviewed experienced at least one mishap or near-mishap while serving on a ship; most of them being near-miss, close quarters situations due to negligence, complacency, training deficiencies, or confusion. While some SWOs expressed that they remained calm and controlled throughout their situations, others admitted to feeling flustered or panicked alongside their watch teams, some instances to include the CO or XO. Several officers also expressed that the pressure of performing sometimes led to putting the ship and crew in precarious situations, even when it was not mission critical or time sensitive.



Not All SWOs Are Created Equal

The professional development of SWOs seems to largely depend on a few random factors. A lack of mentorship was identified as one of the biggest challenges they face, as it seems to be dependent on being in the “right place” at the “right time.” Mentorship was also described to have to be individually sought out up and down the chain of command, suggesting that commands do little to foster mentor-mentee relationships.

Another major challenge identified was the varied standards of qualifications. According to interviewees, there is no real standardization when it comes to training or major qualifications, such as OOD, SWO, EOOW, or TAO. While the PQS system exists, the rigor and standards of qualifications are set at the command level, meaning that the quality of qualifications and professional development are fully dependent on the standards set by the ship’s CO. As a result, officers are developing differently across the fleet, sometimes even within the same wardrooms. Several interviewees expressed concern about “give me” qualifications awarded by their previous COs despite them not being proficient, capable, or knowledgeable enough to “sit the seat.” This approach to professional development helped to “degrad[e] warfighting because it makes being a SWO mean less.”

Lastly, onboard training and drills were seen to differ by experience and priorities. Some interviewees described trainings and drills to be taken seriously and felt that they were effective. However, the majority had contrary views on how their ships conducted trainings and drills, even if that meant sending ships on deployment ill prepared after cutting corners. In their experiences, training and drills were done more so to be able to say a requirement was met (e.g., “check in the box”) rather than to prepare crews for operational employment; some went as far as to describe them as “rehearsals” for inspections and assessments. Most training scenarios were described to be “unrealistic, poorly constructed, and a series of people going through the motions.” One officer believed that “people don’t take it seriously because they don’t truly think that something like this is going to happen.” Another stated that “it’s better to be a warrior in a garden than a gardener in a war, and right now, we are just a bunch of gardeners.”

When questioned why the fleet’s approach to training lacked focus, interviewees across the board believed that there were too many aspects of the job that took away or distracted from effective warfighter development. Administrative requirements, a “zero-defect” mentality, flaws in the maintenance system, unforgiving ship schedules, and deployment rotations were just a few examples. The combination of these distractions was seen to result in ships and crews deploying without the necessary skills to win in a kinetic fight. Many SWOs, including ship captains, expressed that ships are being sent out “administratively ready” but that deployments were the ideal time to conduct actual “effective and realistic training” as there is no pressure from outside entities or competing priorities. Conceptually, however, the ship and crew should already be at their peak capability prior to going on deployment.

SWOs across the board would like to see better and more effective training onboard ships at all stages of the training cycle. They recognized deficiencies the system and believed that improvements in training would make the biggest difference in proper system execution and warfighter mentality development. They believed that the structure of the cycle, the “crawl, walk, run” approach to surface warfare, had a lot of potential to be effective and made sense. However, the execution of this system was widely criticized. SWOs want to see changes to reflect and support realistic, relevant, and serious training met with a motivated and bought-in crew. Departing from the “check in the box” approach could be the most influential shift for warfighter development in the fleet

The Ethics of Readiness

Several officers shared that they, or others close to them, acted unethically in response to external pressures when reporting readiness levels. Even for major certifications like COMPTUEX, both assessors and participants alike described that certain parts of scenarios were sometimes modified to give ships the “green light to deploy.” Due to the overwhelming and compressed training cycle, constant turnover, and undermanned crews, ships are being forced to complete integral training and development at faster rates, making it difficult for SWOs to manage every program simultaneously successfully and effectively. Additionally, the “get it done attitude” was described to be detrimental because “it doesn’t seem like ‘Big Navy’ cares about how we get it done. They just want it done and a green spreadsheet...this leads to



people cutting corners and presenting a false state of readiness to higher ups just to make them happy and to make themselves look like good leaders.”

Interviewees expressed a sense that there was very little room to fail without creating more pain and suffering for the crew; some ships were unable to send their sailors home before deploying for seven to nine months as a result from failure. Therefore, meeting requirements, keeping up with the ship’s operational tempo, and doing it all “in the green” were all sources of stress felt by SWOs, contributing to the “zero-defect” mentality, and, in some cases, unethical behavior.

SWOs Endure Extreme Stress About the Same Things

SWOs across ranks believe that their job-induced stress comes from the same things. Almost every interviewee expressed that they put an immense amount of pressure on themselves to succeed. As many SWOs are described to have “type-A” personalities, having control over their work is comforting. Throughout the interviews, officers often referred to “the grind never stops” mentality and the perpetuated “get it done” attitude. These mindsets have existed in the SWO community through decades of experience, budget cuts, optimization plans, support for landlocked wars, maintenance backlogs, etc. They feel that this pressure, in addition to the tight deployment work up schedule, creates “high stakes” for ship captains and their crews to complete evolutions, drills, assessments, and certifications without fail. Many SWOs feel like they are constantly “burning the candle at both ends.”

Fear of failure seems to contribute to the risk averse culture in the SWO community, which was highlighted as an aspect that degrades the community overall. SWOs expressed a fear of making mistakes as they believed it would negatively affect their career projection. Whether it was a junior officer with aspirations of commanding a warship, a department head close to retirement, or a ship captain eyeing major command or a star, they believe that one mistake or a single bad fitness report could derail their entire careers. According to the officers interviewed, this fear results in the timidity, hesitancy, and micromanagement seen across the community. Not only did they feel that their careers were on the line by their own actions, decisions, and judgments, but by those of their subordinates as well. This kind of pressure was seen to keep SWOs on edge, toxically competitive, and risk averse. While taking the slow, smooth, methodical, and careful approach to operations have kept most SWOs out of shallow waters, it has also left many wondering if they would be able to exercise the grit, toughness, and quick thinking required in times of extremis and threat.

Attraction to the SWO Community

The majority of SWOs interviewed did not originally want to be SWOs, although there were a few distinguishable factors about being a SWO most believed to be favorable. Because SWOs start their service obligation almost immediately, they “hit the fleet” faster than any other community. Unlike pilots, submariners, special warfare operators, and Marines, who go through lengthy training pipelines before entering the fleet, the SWO community traditionally sends their officers straight to ships to begin on-the-job training. Almost every interviewee liked the idea of getting to the fleet sooner. Whether they wanted to start repaying their service obligation right away, set the conditions to laterally transfer to a different community, or bypass lengthy and rigorous training commands, the notion of apprenticing in a job coupled with working with sailors was appreciated by all. Being given the opportunity to lead sailors sooner was particularly appealing and there was a significant theme of servant leadership across ranks. Specifically, a common motivation within the SWO community is to serve and work for the betterment of their subordinates, even when times are tough. This approach to leadership is extremely apparent at the junior officer level.

Mental Fitness is a Priority, Physical Fitness is Not

Physical fitness was seen to be one of the easiest things to ignore when other requirements emerged. Other aspects of the job were often seen to prioritize above physical health, although most officers interviewed believed it to be an integral aspect of warfighting. Not only does physical fitness give one the strength and stamina to run up and down ladder wells, drag shipmates to safety, hold one’s breath under water, fight fires, or stand a watch at General Quarters for hours on end, it also gives you mental clarity, a



relief in stressful times, and an opportunity to push yourself past your comfort zone. Yet, outside of “PRT season” when the Navy conducts physical fitness assessments, physical fitness is not a priority for SWOs. One officer stated that “the state of the fleet in physical fitness shows how much we prioritize the warfare part of surface warfare.” However, some commands were described to have tried to prioritize physical fitness when they could. Those command were subsequently described to have had leadership who were physically fit themselves and who prioritized physical fitness on a personal level.

Conversely, mental fitness was seen to have made strides. The stigma associated with seeking help for mental health has lessened in recent years. With that, the message of taking care of yourself, along with the availability of programs and resources, have become more prevalent. Mental health was generally taken seriously at all levels of the chain of command. However, the attention on mental fitness was believed to be very reactionary. Interviewees believed that there was little to no emphasis put on preventative maintenance or proactively developing mental toughness, fitness, or health. Actively working on mental toughness and cognitive development was identified as another way to bolster the warfighter mentality.

Conclusion

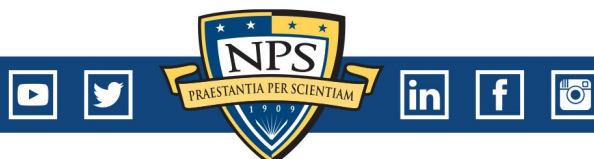
My research indicated that the SWO community could benefit from putting more emphasis on actively developing the warfighter mentality among both junior and senior officers. In my thesis, I make several recommendations for how the community can do this. One of them is to publish doctrine that includes SWO warfighter behavioral and cognitive characteristics. Neither I, nor anyone I interviewed, could recall or locate official Navy doctrine, publication, or manual that explicitly describes the values and characteristics of a warfighter as it pertains to the SWO community, nor how to nurture and develop them.

It is important to standardize the vision for who the Navy wants the average SWO to be as far as leadership and warfighting. Publishing and disseminating the key warfighting tenants that the community values can help directing SWOs in the same direction and focusing commanders and wardrooms in cultivating the SWO warfighter as well as the warfighter mentality as the community intends. Another recommendation is to standardize the qualification process in the SWO community. This would ensure that each SWO is being trained and assessed by the same rigorous standards across the fleet at all levels. While on the job training is an integral part of experience and practical knowledge, the difference in the quality of training throughout the fleet was apparent, particularly when considering one’s duty stations, coasts, or countries.

The SWO community has historically been seen as a “catch all” community as it seemingly does not require great skill or aptitude to join the community. There does not seem to be as much prestige or allure in comparison to other communities. Those who fail out of other programs like flight school or nuclear school end up redesignating as SWOs, creating the perception of “those who can’t... become SWOs.” As much as the Navy has tried to revitalize the community’s reputation, it is not as desirable as other communities with higher standards. Creating a rigorous training pipeline to include shipboard watch station qualifications would not only help rehabilitate the community’s reputation, but it would also raise the baseline level of knowledge of the SWO community, delivering ready and capable officers who are ready to contribute to the team the moment they step on their ships.

The divide between the perception and the assessment of readiness amongst the different ranks of the SWO community is particularly interesting as they all serve in the same Navy, on the same ships, and, when the time comes, will inevitably go into battle together. The mentality of wanting to do good work, doing it right the first time, every time, and having high expectations speaks highly to the thoroughness and dedication of SWOs in general. These are qualities, if shaped and aimed in the right direction, can do more help than harm in the community. Focusing on operational development, quality training, and incorporating the “why” in everything that they do can bring SWOs that much closer to the fight and ultimately closer to triumphantly demonstrating naval superiority against any threat across the globe.

LT Judith Hee Rooney is a Human Resources officer currently serving as the Enlisted Programs Officer for Naval Talent Acquisitions Group New England. Previously, LT Rooney served as a SWO onboard USS KEARSARGE (LHD-3) as the Damage Control Division Officer and the Internal



Communications Officer and onboard USS WINSTON S. CHURCHILL (DDG-81) as the Assistant Chief Engineer. She got her Master of Science in Manpower Systems Analysis from the Naval Postgraduate School where she won the Surface Navy Association's Award for Excellence in Surface Warfare Research for her thesis: *The State of the Warfighter Mentality in the SWO Community*.

[The State of the Warfighter Mentality in the SWO Community | Center for International Maritime Security \(cimsec.org\)](#)

[The State of the Warfighter Mentality in the SWO Community | RealClearDefense](#)

[Return to Index](#)

STUDENTS:

SOF and Field Sanitation: The Importance of a Healthy Partner Force

(Small Wars Journal 30 Aug 22) ... Maj. Pete Reider

The development and implementation of effective field sanitation and hygiene procedures marked a revolutionary step in battlefield technology. It marked a critical turning point in the early 20th century when the number of soldiers killed from disease an infection was proportionately less than those who died in or were wounded through combat. US planners began to address this problem following the First World War and it was at this point the US transitioned, as Vincent Cirillo notes, from the disease era to the trauma era.

But the threats of the “disease era” are not confined to the past. Question of sanitation and health are vital consideration when working with developing and underdeveloped partners forces today. Many of the partners that the US currently works with have lower initial levels of health due to multiple environmental and educational factors within their countries. It is critical for the modern-day SOF commander working with partner forces to understand the importance of proper implementation of field sanitation and hygiene, and in particular to consider insecticides and protective wearing of clothing.

Case Study of The North Africa Campaign

During the 1943 North Africa Campaign, allied forces faced outbreaks of typhus, bubonic plague, and malaria. These outbreaks drained units of men and preoccupied numerous medical units. These diseases were mitigated through the application of pesticides including Dichlorodiphenyltrichloroethane (DDT). The North African campaign could have suffered significantly from civilian and military outbreaks of the disease if the US did not possess the technology and institutional ability to employ DDT effectively.

A high percentage of diseases are transmitted through carriers known as vectors, typically anthropoids or small mammals. These vectors spread disease through a given area by carrying it on or within their bodies. The effective means of limiting or eliminating vectors are either the destruction of habitat or the annihilation of the vector. Disease rates among US troops significantly dropped when DDT was used in North Africa. Patients requiring hospitalization between July and September of 1943 were approximately 21,482, versus 17,375 patients that were hospitalized for combat sustained injuries. The use of aerosol DDT was started in August of the same year and continued until 1945. Over a two-year use of DDT, cases of malaria, transmitted by mosquitoes, dropped from a high of 32,811 cases down to 5,765 cases.

Despite the measures of effectiveness, DDT was outlawed a in 1972 due to its carcinogenesis nature and ecological implications. The military retained the use of DDT for “emergency use” applications due to the lack of an effective replacement. The lesson of DDT and its effects were clear despite its toxicity: military forces in the future must effectively utilized field sanitation methods for force preservation.



Contemporary use of Insecticides in Modern Conflict

The United States military no longer relies on the mass spraying of areas of operation as it did with DDT. The modern system of insecticide use now resides at the individual level. The military uses a multipart system to apply repellants. Uniforms are impregnated with an insecticide (permethrin) and periodically treated with a 40% permethrin solution. This repellency lasts throughout the lifecycle of a uniform. An aerosol spray can of permethrin is available and will last approximately five to six washes if the uniform does not come pretreated. This option provides flexibility to units that may not wear standard uniforms and partner forces who do not have access to treated uniforms.

The ease of use of systems can be intuitive for western forces and for partner forces with some training. The current system provides adequate protection but relies on diligence of those using it. The washes and creams are easy to transport, shelf stable, and relatively inexpensive. Once the insecticides are in theater, soldiers can effectively use them without the need for an occupational specialist. The simplicity of the systems allows for the ease of training partner forces in their use. The disadvantage of this individual level use is that it requires leadership of US and partner forces to ensure they are being used properly. The effectiveness of modern pesticides can be negated by soldiers' lack of diligence in proper use, not receiving proper training, or not using them altogether.

Current systems are the best solution and provide ease in application for SOF. The flexibility, low cost, and durability makes for an attractive solution for partner forces. SOF training and equipping partners with these preventative measures, creates immediate benefits. Partners will have a higher readiness rate due to less fighters stricken with disease. There is a lessened requirement for medical assets; SOF teams are task-saturated, and resource limited. Preventing diseases in an expeditionary environment preserves medical assets for trauma response. Healthy partner forces also preserve the health of the SOF who work with them. Diseases will travel regardless of national affiliation when confined to small areas such as a combat outpost. The overall footprint of SOF may also be kept at a minimum necessary level because the lower the number of potentially sick soldiers, the lower the required number of forces to accomplish the mission.

The prevention of disease among allies or partner force may have secondary and tertiary effects in addition to preserved combat power. When partner forces are educated in the use of field sanitation the benefits not only impact the military forces but extend into the local community. This safeguards the community from communicable disease, which may achieve a positive effect in the morale of the partner force and perception of US forces overall. When partner forces' families are healthy, it increases their morale and willingness to conduct operations. Conversely, this may be used as a tool for the United States to legitimize a partner force or partner government by increasing the overall health of the population.

The system of application to clothing, equipment, and exposed skin is extremely easy to understand even for the most rudimentary partner force. These simple measures may provide significant improvements to disease prevention

Conclusion

A commander cannot understate the importance of a healthy fighting force, especially an indigenous force. In special operations relying on the indirect approach, mission success will depend on the partner force's military effectiveness. A rudimentary part of effectiveness is their physical ability to fight which encompasses being healthy enough and having enough of the force available quantitatively for conducting operations. The easiest way to preserve combat power is to prevent disease. This level of readiness can be achieved through simple preventative measures such as the use of insecticides and keeping areas free of debris that will attract vectors of disease. The US can preserve not only our own combat power but the power of our partner forces while conducting special operations in adverse operational environments by observing by adhering to basic field sanitation.

MAJ Pete Reider is a active duty Civil Affairs Officer, with multiple deployments to the CENTCOM AOR. He is currently a graduate student at the **Naval Postgraduate School** studying defense analysis.

[SOF and Field Sanitation: The Importance of a Healthy Partner Force | Small Wars Journal](#)

[Return to Index](#)



FACULTY:

Uncertain Outcomes Will Likely Result From China's Military Display Over Taiwan

(English News Track 23 Aug 22) ... Aniket Dixit

China: The world's largest standing army was able to test the coordination of its personnel, weapons, supplies, and communications thanks to China's massive intimidation campaign this month in response to US House Speaker Nancy Pelosi's trip to Taiwan, although the results are not entirely clear, analysts said in Washington on Monday.

The People's Liberation Army was overhauled in 2016, and this military show of force required cooperation from the army, navy, air force, and logistics branches. It was the largest since that time. The PLA hasn't always been well-coordinated and has historically been led by the army.

According to analysts at a Center for Strategic and International Studies event, Beijing praised PLA forces' close cooperation in the face of recent tensions, along with evidence of easier logistics involving army long-range artillery and missile units under the military's Eastern Theatre Command.

According to Roderick Lee, research director at Air University's China Aerospace Studies Institute, "If the army and rocket force fires were coordinated, that would suggest some level of joint command-and-control at the theatre level," which is the impression Beijing wants to convey. "The actions we're witnessing are definitely meant to send a message and to deter."

However, it was still unclear how much progress had been made in terms of integration as a whole. The mistakes made by Russia since it invaded Ukraine in February serve as a reminder of the importance of coordination for military performance.

The PLA hasn't tested some capabilities, such as sustained artillery bombardment or blockading ships in the waters surrounding the island, which it would probably need for an actual invasion of Taiwan. The unprecedented exercises China conducted this month highlight the country's increasing reliance on "grey-zone" strategies, which involve combining military and non-military operations. To make its point, it employed coercion in the areas of economic, financial, informational, and cyberspace.

Beijing specifically launched drones over Taiwan's Quemoy archipelago, also known as Kinmen, just off Fujian province, banned some Taiwanese trade, slammed US and European nations that expressed concern over its actions, and waged disinformation campaigns in addition to its various military actions.

Cristina Garafola, a policy researcher at the Rand Corporation, said: "What we're seeing is generally consistent with China's grey-zone approaches." "That's likely to continue moving forward, along with these kinds of grass-roots pressure efforts to change the perception in Taiwan society,"

The analysts added that Beijing's display of force in response to US House Speaker Nancy Pelosi's visit to Taiwan this month has set a new baseline that could see China's military react even more forcefully to perceived future transgressions.

The PLA would need to inflame tensions even more the next time to prove it means business after breaking several rules by sending record numbers of ships, military aircraft, and drones into and around Taiwan, holding lengthy live-fire drills, and launching missiles over the island and into Japan's exclusive economic zone.

According to M Taylor Fravel, director of the Massachusetts Institute of Technology's security studies programme, "I've got to believe another shoe will drop, one way or another." In other words, "I don't think the genie can be put back into the tube."

China sees Taiwan as a separatist province that should, if necessary, be reunified through force. The self-governing island is not recognised as an independent state by many nations, including the United States. Washington's strategy, however, is to support Taiwan's ability to defend itself militarily as well as its increased influence in international affairs such as crime, health, and aviation, which Beijing opposes. The United States' immediate response will determine a lot of things. The Pentagon has so far resisted verbally but only carried out military drills that were pre-planned before California Democrat Nancy Pelosi's arrival in Taiwan on August 2.

However, the US navy will want to avoid coming off as complacent or appearing to accept Chinese military vessels entering Taiwanese waters after crossing the median line. That could then start a potential



escalation cycle of tit-for-tat. Christopher Twomey, an associate professor at the US **Naval Postgraduate School**, stated that "this is most likely the early stages of a crisis that is going to continue to percolate for months."

It will be crucial for us to convey to both China and our allies that we won't be deterred from exercising our rights to freedom of navigation and that the US Navy will respond in a provocative manner as a result of these exercises.

Another issue is the talking points coming out of Washington. Following Beijing's vehement opposition to Pelosi's visit, President Joe Biden's administration adopted the stance that China had manufactured the crisis and overreacted, claiming that numerous US lawmakers had already visited Taipei and that everything should go back to normal.

Analysts noted that this tactic runs the risk of making Beijing feel as though its concerns are being disregarded and that its signals have not been taken seriously.

The coming political calendar for the various parties to the tensions is packed with important dates, which only serves to complicate matters. President Xi Jinping is anticipated to win a third term at China's 20th Party Congress, which is currently being prepared for. Taiwan will hold local elections while the US will hold its midterm elections.

Additional official visits, US trade negotiations with Taiwan, US legislation like the Taiwan Relations Act, and additional arms sales are among the unresolved issues that Beijing views as US provocations.

According to Garafola, Taiwan's ruling party has refrained from labelling the recent developments as a crisis. This is a result of President Tsai Ing-wen's desire to promote more visits to the island in order to increase its visibility abroad.

Therefore, if they discussed a crisis that resulted from one of these visits, Garafola said, adding that a variety of factors were at work. "This is the beginning of something where we could see more potential flashpoints," the author said.

[Uncertain outcomes will likely result from China's military display over Taiwan | NewsTrack English 1 \(newstracklive.com\)](https://www.newstracklive.com/uncertain-outcomes-will-likely-result-from-china-s-military-display-over-taiwan)

[Return to Index](#)

As China's Navy Grows Ever Larger, So Does the Threat to Taiwan

(Japan Times 25 Aug 22) ... Gabriel Dominguez

(Transcontinental Times 25 Aug 22) ... Gabriel Dominguez

As Beijing ramps up military activities around Taiwan, the steady growth and modernization of China's naval fleet is fueling concerns about how Beijing could use what is already the world's largest navy in a move against the self-ruled island.

The People's Liberation Army (PLA) Navy could not only play a crucial role in blockading and attacking the island, but also in attempting to deter and deny a potential intervention by the United States and its allies during such a campaign — a concept known in military parlance as “anti-access/area denial.”

Crucial to this is not only the increasing capabilities of Chinese warships and associated systems, but also the impressive rate at which they are being constructed.

China is the world's top ship-producing nation by tonnage and nearly self-sufficient in all its shipbuilding needs. This capability, which is being enhanced through shipyard expansions, was highlighted late last week when an image emerged on social media showing five new Type 052D guided-missile destroyers being built at the Dalian shipyard in northern China — one of two major facilities building large surface combatants.

This destroyer class “is the culmination of substantial experimentation in ship design by the PLA Navy over the preceding decades. With the 052D, the Chinese have finally found a design they are satisfied with, and they have been engaging in serial production in recent years, with over 14 currently in



the fleet,” said Christopher Twomey, assistant professor of national security affairs at the U.S. **Naval Postgraduate School** in Monterey, California, emphasizing that he was not speaking on behalf of the U.S. Navy.

Exponential growth

The PLA Navy has grown exponentially, with the fleet expanding by 132 warships over the past 17 years to make it the largest in the world by number — about 65% of this growth was the result of increases in missile-armed fast patrol craft and corvettes. The rate of warship production has been so high that, between 2017 and 2019, China reportedly built more warships than India, Japan, Australia, France and Britain combined.

In last year’s China Military Power report, the Pentagon stated that China had an overall battle force of approximately 355 ships and submarines, while the U.S. Congressional Service put the figure slightly lower at 348. In comparison, the U.S. Navy’s battle force was approximately 296 ships as of 2021.

Last year alone, China commissioned at least 28 warships, while the U.S. Navy inducted only a handful of vessels, the Washington-based Center for Strategic and International Studies (CSIS) noted in a report. China could have 425 combat-ready ships by 2030 should it continue to commission vessels at a similar rate.

“The Chinese navy is growing at a much faster rate than any other large navy, and more crucially, it is modernizing,” said naval analyst and writer H. I. Sutton. “There may be challenges ahead such as China’s aging population and the increasing cost of maintaining what has already been built, but the expansion is likely to continue.”

The PLA Navy of the 2030s might be almost as unrecognizable as today’s is from 10 years ago, he added.

But while the PLA Navy is expanding its quantitative lead, the U.S. Navy still maintains a substantial qualitative edge, although Beijing is seen to be closing the technological and capability gaps in many areas.

“The U.S. fields far more capable aircraft carriers and other large surface combatants, while China fields many smaller vessels. This means the U.S. Navy also has an edge when it comes to overall firepower,” said Brian Hart, a fellow with CSIS’s China Power Project.

That said, U.S. naval forces are globally distributed, while China’s naval power is largely concentrated along its maritime periphery.

But it is not just the number of vessels. Beijing is also modernizing naval systems and weapons, with the Pentagon stating that the PLA Navy will have the capability to conduct long-range precision strikes against land targets from its submarine and surface combatants “in the near term” using cruise missiles.

China is also enhancing its air defense, anti-ship and anti-submarine warfare capabilities and competencies to protect its aircraft carriers and ballistic missile submarines.

Threat to adversaries

So, what could this mean for Taiwan?

By modernizing and increasing the size of its navy, China aims to be capable of achieving a greater degree of control over its near-seas region, while defending its commercial sea lines and keeping U.S. and allied forces at bay, if required, during a Taiwan contingency. Failing that, the navy — supported by other military services — should at least be capable of delaying the arrival or reducing the effectiveness of intervening U.S. forces.

“Today, China is far more capable of projecting power around Taiwan, and the PLA has sought to demonstrate that with its recent unprecedented exercises,” Hart said.

China’s large quantity of ships and submarines could be used to saturate the Taiwan Strait and other waters around the island, Hart explained.

“The PLA Navy’s increasingly sophisticated fleet of submarines would play a particularly important role in holding adversary navies at risk. Destroyers and other major surface vessels could be called upon to implement a blockade and interdict ships seeking to break that blockade,” he said.



Sutton added that the PLA Navy could also interdict efforts by other countries to resupply Taiwan while holding many of its own ships in reserve. A large fleet also means that China could afford to take greater losses, in stark contrast to the Russian Navy amid its invasion of Ukraine.

At the same time, large amphibious vessels would be crucial to the PLA's efforts to land troops and equipment onto the island if China were to move forward with an invasion.

However, Twomey explained that these ships are highly vulnerable to an attack, and China currently does not have enough of them to conduct and support an amphibious assault on Taiwan. This is why Beijing has begun testing the use of commercial ferries for transporting personnel and equipment while employing military vessels as armed escorts.

According to the Pentagon, the PLA's anti-access/area denial capabilities are currently the most robust within the so-called First Island Chain, which extends from the Kuril Islands to Borneo. However, China has begun fielding significant assets for operations much further out.

The most relevant new assets being deployed by the Chinese navy to fulfill such missions are improved submarines, long-range anti-ship missiles and large surface combatants. These last kinds of vessels are being equipped with a range of advanced systems, such as air defense and anti-submarine weapons, and could begin fielding hypersonic anti-ship missiles.

Taiwan's asymmetric response

In response to the growing risk of a cross-strait military conflict, the leadership in democratic Taiwan has been enhancing the island's self-defense capabilities and strengthening relations with friendly countries, particularly the United States.

In the words of Taiwanese President Tsai Ing-wen, the island's strategy is to make "invading Taiwan or trying to invade Taiwan something that is going to be very costly for China."

To achieve this, Taipei has been increasing military spending since 2017. On Thursday, the government proposed a record 415.1 billion New Taiwan dollar (\$13.72 billion) defense budget for 2023, a rise of 12.9% year-on-year. On top of that, Tsai's Cabinet is seeking an additional NT\$108.3 billion from parliament for more fighter jets and other sea and naval assets.

To make best use of the island's limited resources, Taipei has been implementing the so-called Overall Defense Concept (ODC) as its main strategy to deter and, if necessary, defeat a full-scale PLA invasion.

Among other things, the ODC emphasizes the use of both conventional and asymmetric capabilities, the latter of which will play an increasingly critical role as Taipei shifts away from the notion of engaging in a traditional war of attrition against the much larger and more capable PLA.

The idea is to field lethal weapons that are difficult to both target and counter by the enemy. Some of these include large inventories of low-cost, short-range precision-guided munitions, fast-attack craft, small missile assault boats, as well as sea mines and fast minelaying ships.

According to the ODC, these asymmetric weapons are not meant to replace the more traditional capabilities, but rather to complement them.

Some of those capabilities are already being provided by the U.S. For instance, Washington is selling anti-ship missiles and Stinger man-portable air-defense systems, while it has approved the sale of High Mobility Artillery Rocket Systems, or HIMARS — which have gained attention during the Ukraine conflict — as well as air-launched cruise missiles and strike-capable drones.

At the same time, the ODC implies the strengthening of Taiwan's defense-industrial capabilities, with Taipei spending more on developing and producing its own military equipment, including indigenous submarines, new minelayers and fast missile corvettes armed with anti-ship missiles.

'Archipelagic defense'

Whether this approach will be ultimately enough to withstand a full-scale Chinese attack is unclear, which is why the United States and its allies are also examining alternative strategies to assist Taiwan militarily.



One proposal would involve turning the anti-access/area denial strategy back against China by equipping relevant islands in the region with mobile, ground-launched anti-ship missiles, as well as air and missile defense systems.

Rather than matching Beijing ship-for-ship and risk losing forces to China's anti-access/area denial capabilities, this "archipelagic defense" concept could make for a lethal but affordable combination — particularly after the collapse of the Intermediate-Range Nuclear Forces Treaty, allowing the U.S. to deploy land-based missiles with ranges of up to 5,500 kilometers — Lyle Goldstein, director of Asia engagement at the Defense Priorities think tank, wrote in an analysis.

However, Goldstein warned that such an approach could also prompt a more offensive-oriented Chinese strategy and face enormous political hurdles, as other countries would not want their territories to potentially become targets.

Goldstein is not alone in thinking this.

"While there are many small islands in the Pacific, those most useful would be the major islands in Japan and the Philippines," Twomey said. "Getting their political support for U.S. deployments is extremely challenging in the current environment."

[As China's navy grows ever larger, so does the threat to Taiwan | The Japan Times](#)
[China's Modernized Navy Begins to Efface Imaginary Taiwan Strait Median Line — Transcontinental Times](#)

[Return to Index](#)

Restraining Russian Ransomware

(FPRI 25 Aug 22) ... Scott Jasper

Last May, Americans up and down the East Coast waited in long lines for gas. The panic wasn't caused by a foreign war or sanctions—it was triggered by a Russian ransomware attack. The Russia-based criminal group DarkSide had infected Colonial Pipeline with ransomware and demanded millions of dollars to unlock Information Technology systems. Colonial shut down the flow of fuel from the Gulf Coast for a week, even after paying the hackers roughly \$5 million.

Soon after, DarkSide went dark when its blog site and payment server were taken down by its service provider. However, the group adapted. It rebranded as BlackMatter in an attempt to avoid law enforcement. That tactic worked until Russian authorities arrested a DarkSide hacker behind Colonial Pipeline in January after President Joe Biden asked President Vladimir Putin to crack down on Russian cyber criminals.

Another prolific ransomware operation named Conti, run by a Russian cybercrime syndicate, chose a different, more clever strategy to continue its operations in the face of efforts by law enforcement to stop them. Conti drew undue attention after the Russian invasion of Ukraine by officially announcing full support for the Russian government, and declaring that it would strike back at the critical infrastructure of any country that decided to organize war activities against Russia. In response, an infuriated Ukrainian security researcher leaked thousands of internal Conti messages and the source code for the Conti ransomware encryptor and decryptor.

Within months, the Conti operation shut down its public facing internet sites used to leak data and negotiate with victims. Instead of a major rebrand, the Conti syndicate continues to operate with gang members splintered into smaller cells that infiltrate other ransomware operations, known as BlackCat, Hive, and HelloKitty. This prevented the whole network from being taken down at once by the authorities. The groups take advantage of the penetration (break into the device) testers (that probe for system weaknesses), developers, and programmers still loyal to the Conti syndicate, gaining access to seasoned expertise and vulnerability exploits. Other syndicate members have created their own data extortion operations that do not encrypt data, such as Karakurt.

Despite the public exposure, Russian ransomware groups have been able to adjust strategies in order to survive. Previous attempts to coerce the Russian government into cracking down on hacker groups on



their own territory have produced only superficial results—Russia did make some arrests of lower-level hackers, primarily for political theater. Even if Moscow had done more, it would be impossible now given the dismal relations between the United States and Russia over the war in Ukraine.

With this level of resilience to continue operations, how can the United States restrain Russian ransomware? America's strategy is to disrupt ransomware actors' activities, finances, and infrastructure. Washington can pursue criminal charges against Russian ransomware with assistance and insight from the intelligence community. The Justice Department has already stepped up efforts to impose costs through arrests of ransomware actors and seizure of their proceeds.

US Cyber Command and the National Security Agency have enabled cross-government actions by sharing key insights on ransomware actors in near real-time. Their commander recognizes that Russian protected gangs carrying out ransomware attacks are a national security issue. Yet as criminals, they operate based on financial motivations. While the government is doing what it can to prosecute cyber criminals, American companies and organizations have no choice but to protect their networks to avoid becoming a victim.

What the Government Can Do

Well before Russia's war against Ukraine, Biden asked Putin to rein in ransomware gangs operating from Russian soil. Biden warned him in Geneva in June 2021 that the United States would respond to attacks on US critical infrastructure. Biden gave Putin a list of sixteen areas that the United States considers off-limits.

In July 2021, the REvil ransomware group, based in Russia, hacked into Kaseya, a Miami-based software supplier for technology service providers. REvil had attacked meat processor JBS USA a couple of months prior, disrupting the distribution of beef and pork for days. However, Biden discounted the Kaseya attack, saying "the impact on US businesses appeared to be minimal." Months later, Russia took steps to take down ransomware attacks emanating from Russian territory. In January 2022, the Russian Federal Security Service, the FSB, claimed that they arrested REvil members and seized funds from more than two dozen residences at the request of US authorities.

One year after Geneva, relations between Washington and Moscow are perhaps at an all-time low in the post-Cold War period. Any hope for a predictable and stable understanding on cybersecurity and ransomware has fallen apart. Dialogue and cooperation today are virtually non-existent on strategic stability matters, such as arms control and cyber attacks. The imposition of significant new sanctions to hold Putin accountable for the invasion of Ukraine dominated the recent G-7 leader meetings. While economic measures intended to deprive Russia of resources necessary to wage war are already imposing drastic costs. Thus, the deterrence levers of diplomacy and sanctions are somewhat spent when it comes to ransomware. Instead, US security agencies warn of Russian criminal cyber threats to critical infrastructure as a response to the unprecedented economic cost imposed on Russia. They pose a threat primarily through deploying ransomware or conducting distributed denial of service attacks that overload websites.

The United States is left with some options to impose costs directly on Russian ransomware gangs. Authorities can go after the actor, their money, or their infrastructure. The legal instrument proved successful in the arrest of Yaroslav Vasinskyi, a REvil operator, responsible for the ransomware attack against Kaseya. Vasinskyi was apprehended in Poland in November 2021 to face extradition to the United States. The Justice Department also announced at the same time the seizure of \$6.1 million in funds traced to REvil ransom payments received by Yevgeniy Polyanin, a Russian national.

Likewise, earlier in June 2021, the department announced it seized \$2.3 million in cryptocurrency paid to DarkSide for the Colonial Pipeline ransom demand. The FBI was able to track multiple transfers of bitcoin to a specific address for which they had the private key to access the assets. The US government is currently offering a reward of up to \$15 million for information leading to the identification and location of the leaders of the Russia-based Conti syndicate. The same offer goes for leaders of Darkside and variant rebrands.

Deputy Attorney General Lisa Monaco says the Biden administration strategy has shifted to rely less on solely charging foreign hackers who may never see the inside of a courtroom. Her remarks came



after US law enforcement disrupted a North Korean state-sponsored ransomware operation using a strain dubbed Maui and recovered about a half-million dollars in ransom payments by hospitals and medical facilities. Monaco says the new strategy is to dedicate resources to disrupt and dismantle malicious cyber activity. This approach uses all available tools and centers on private sector reporting and collaboration.

Embracing a strategy to disrupt and dismantle the activities of cyber criminals would allow law enforcement, in theory, to follow the money, extract decryptor keys, and prevent the next victim. In practice, disrupting cyber activity is easier said than done. Not only are many cyber actors out of reach of US authorities, but their infrastructure might be inaccessible, too. The hosting provider that agreed to shut down a DarkSide server was in New York, whereas a server provider for Conti that supports anonymous payment methods is located in Russia. The provider named Inferno Solutions says that they always side with the client and “do not disturb clients in case of dubious and unlawful complaints (abuse).”

Playing Defense

To protect companies and organizations from ransomware attacks, the United States has already embraced boundary firewalls, strong passwords, and vulnerability patch management. In addition, critical infrastructure entities in particular should segment networks, enforce multifactor authentication, and adopt endpoint (any physical device that can be connected to a network) and detection response tools.

Conti partners have also deployed the ransomware against US healthcare and first responder networks. These are tempting targets for ransomware criminals because they are eager to restore services and therefore likely to pay the ransom. The potential for lucrative payouts is a stark reminder that beyond advancing the interests of the Russian state, Russian ransomware groups are relentless to obtain financial gains.

Targets of ransomware have no choice but to harden their defenses. US security agencies routinely provide technical details and suggested mitigations in their joint cybersecurity advisories on these groups. For instance, an advisory on Conti ransomware describes twenty-three techniques routinely employed by Conti actors, along with what is called the MITRE ATT&CK framework adopted by industry and the government. Going forward, Conti syndicate members will undoubtedly use these same methods to gain access, move across networks, evade detection, and impact targets by data encryption.

Mitigations are meant to help network defenders reduce the risk of compromise by ransomware attacks. It’s common for companies and organizations to require multifactor authentication and strong passwords to remotely access networks, and implement block lists to prevent users from reaching nefarious websites. In addition, ensuring network segmentation helps prevent the spread of ransomware, and maintaining offline encrypted backups of data assists recovery efforts. Finally, upgrading software and scanning for vulnerabilities or flaws that actors could misuse for code execution is part of a strong cybersecurity strategy.

FBI FLASH reports also disseminate identified techniques and indicators of compromise associated with ransomware variants to cyber security professionals and system administrators. A FLASH on BlackCat ransomware revealed that cyber actors leverage Windows scripting language (PowerShell and Batch) to deploy ransomware, and leverage Windows administrative tools during compromise. These observed methods reinforce recommendations for organizations to implement an endpoint and detection response tool for identifying abnormal activity.

US Military Cyber Operations

In recent congressional testimony, General Paul Nakasone, the head of US Cyber Command and the director of the National Security Agency, declared that ransomware can have strategic effects, citing the disruption of Colonial Pipeline. He referenced that incident when telling participants at the 2021 Mandiant Cyber Defense Summit that “when ransomware affects critical infrastructure, it’s a national security issue.” This is even more the case if ransomware attacks are carried out by criminal gangs that are protected by the nation-states in which they live, specifically Russia. In response, Nakasone told Congress his command has taken numerous actions over the past year to combat ransomware. They have worked with interagency and industry partners to disrupt and degrade the operations of ransomware groups that attack critical infrastructure. One of the goals of their actions is to impose costs on these



criminal gangs, which according to Nakasone is “an important piece that we should always be mindful of.”

The first and really only publicly reported action by the US military against a Russian ransomware gang occurred in October 2021. US Cyber Command blocked the website of the Russia-based REvil ransomware group by diverting its traffic. This operation deprived the group of the medium they used to extort and negotiate ransoms from victims. Cyber Command redirection of the traffic was enabled by information on servers and private keys shared by the FBI. Within hours after the Cyber Command operation, a REvil leader wrote “Domains hijacked from REvil” on a Russian language forum. Then he wrote “they are looking for me” and “Good luck everyone. I’m taking off.” Soon after REvil stopped operations, at least temporarily. The REvil disruption was clear evidence that ransomware operations will be treated as risks to U.S. national security.

US military and law enforcement operations have forced top-tier Russian gangs to shut down. IBM security unit X-Force states seventeen months is the average time before a group disappears and reemerges under new names. BlackCat rose from BlackMatter after police pressure and a decryptor was created and used by the security firm Emsisoft to help victims recover files. Gang members confirmed in an interview they are affiliated with DarkSide and BlackMatter. BlackCat was blamed for a ransomware attack on two German oil companies in January 2022 that affected hundreds of gas stations across Germany. Other rebrands, like GrandCrab switching to REvil, after arrest of affiliates, depict a vicious cycle.

Looking Ahead

Before Conti disbanded into splinter cells, US security agencies warned in March 2022 that Conti ransomware has been used in more than 1,000 attacks against US and international organizations. At that time, BlackCat had breached at least sixty organizations worldwide, and those included victims in construction, transportation, insurance, telecommunication, and pharmaceuticals. The targets of Russian-protected ransomware gangs constitute a national security issue. Yet even before the invasion of Ukraine, the Russian government did not seriously crack down on ransomware operators. The raid on REvil was a political stunt during security talks. Russian security services arrested low-tier members who were only charged with “illicit money control/ laundering”—not hacking.

US law enforcement and the military are left to chase down the actors behind ransomware, their money, and their infrastructure. Russian-linked groups are invariably going to become more sophisticated and more evasive over time. BlackCat. Is the first ransomware group to code their encryptor in Rust, a more secure and highly customizable programming language that facilitates the ability to pivot and individualize attacks.

The technical innovations and rebrands made by ransomware gangs will require the US government to take a proactive approach focused “from every angle” to restrain Russian ransomware. As the Colonial Pipeline incident demonstrated, an effective ransomware attack can undermine the economy and upend domestic politics. The best defense for American companies and organizations, therefore, is to harden defenses with procedures and tools suggested by government security agencies.

Scott Jasper is a senior lecturer at the **Naval Postgraduate School** in Monterey, California, and the author of "Russian Cyber Operations: Coding the Boundaries of Conflict" by Georgetown University Press.

[Restraining Russian Ransomware - Foreign Policy Research Institute \(fpri.org\)](https://www.fpri.org/restraining-russian-ransomware)

[Return to Index](#)



The Fourth Taiwan Strait Crisis is Just Starting

(War on the Rocks 22 Aug 22) ... NPS Christopher P. Twomey

The Chinese military exercises that began on Aug. 3, 2022, have initiated the Fourth Taiwan Strait Crisis. The most immediate reason for this was Speaker Nancy Pelosi's visit to Taipei. But this is a bigger crisis, driven by bigger factors. There has been a steady erosion in Sino-American relations and — not unrelated — a shift in the nature of U.S.-Taiwan relations that Beijing finds deeply threatening. As a result, expectations of a rapid resolution to the crisis are chimeric, as too are blithe expectations of a quick return to the status quo ante.

Like the previous three Taiwan Strait Crises, this will likely mark a turning point in Sino-American relations. As in previous crises, domestic political dynamics among all three participants will drive opportunism and complicate crisis management and diplomacy, extending its duration. This creates further potential for misperceptions, miscalculations, and mistakes, all increasing the risk of inadvertent escalation. Leaders in Beijing, Washington, and Taipei should recognize the dangers inherent in this crisis and engage in both selective restraint and cautious diplomacy.

Origins of the Current Crisis

All the previous Taiwan crises had important implications for regional security, and we should expect the same today. The First Taiwan Strait Crisis of 1954-1955 had the most potential to escalate. It involved intense shelling of offshore islands, nuclear saber rattling by the United States, and successful amphibious operations by the People's Liberation Army that led to the seizure of several small islands. The Second Taiwan Strait Crisis, in 1958, involved such bravado from Mao Zedong that even Soviet leader Nikita Khrushchev was put off, contributing to the Sino-Soviet rift. The Third Taiwan Strait Crisis erupted out of Chinese anger at Taiwanese President Lee Denghui's visit to the United States in 1995. Although it arguably had limited potential to escalate given the relevant military balance across the Taiwan Strait at the time, there were major implications nonetheless: It sparked double digit growth in China's military budget and led the People's Liberation Army to develop anti-access, area-denial doctrines to threaten U.S. carriers deployed during future incidents. When it is finally resolved, the current crisis will likely have had similarly significant effects.

Thankfully none of the previous crises escalated into a major Sino-American war, and there are reasons to be hopeful that this crisis will not either. China has a great need for stability in the run up to the Party Congress in the fall, and Beijing recognizes that initiating a military offensive would be highly unpredictable.

Nonetheless, we are in the early stages of the Fourth Taiwan Strait Crisis: It is likely to continue for weeks and months and even now it is more severe than the third. Already, events have surpassed important thresholds. Some five to nine missiles passed over Taiwan en route to targets east of the main island. Portions of two of the initial exercise boxes fell within territorial waters claimed by Taiwan, and one comes within just a few miles of a small Taiwanese island. The initial set of six declared boxes bracket the island as a whole and key ports, much more than the closure zones in 1995 and 1996. Five missiles targeted areas within Japan's claimed exclusive economic zone beyond those that China disputes. Although violations of Taiwan's air defense identification zone have become more common in recent years, they too have intensified in the past weeks. Chinese helicopters have buzzed Taiwan's offshore islands, two Chinese carriers have been put to sea, and additional exercises have been announced.

Beyond China, the military involvement of other actors has also been significant. The United States has gathered substantial naval capabilities in Northeast Asia, far more than a routine deployment. According to the U.S. Naval Institute, of the 114 ships currently operationally deployed across the entire globe, 59 are attached to the Seventh Fleet, the forward-based fleet originally ordered to patrol the Taiwan Strait in 1950. This includes one super carrier and two smaller carriers, with an additional super carrier and another smaller carrier finishing Rim of the Pacific exercises near Hawaii. All of those are capable of launching F-35 strike aircraft. Beyond this, a B-2 taskforce is deployed in Australia, a rotational deployment of F-35s arrived in Korea last month, and a 12-day command and control exercise centering on the Southern Pacific began on Aug. 3. Some of these deployments may have been long planned



(China's carrier deployment may have been as well). But others, including one of the small carriers put to sea in recent days, are clearly reactions to Chinese escalations. The result is a major concentration of forces available to monitor the situation surrounding Taiwan. And on top of all this, an additional congressional delegation visited the island later in the month.

Of course, Taiwan's military is also monitoring the situation and on high alert. The overflight of Taiwanese airspace obviously increases the need for monitoring and the potential for direct engagement of forces. During China's exercises, Taiwan's Ministry of National Defense announced that its missile defense capabilities "have been activated." In addition to conducting pre-scheduled exercises aimed at repulsing amphibious assaults, other capabilities are in higher states of readiness as well. Finally, Japan's military has actively monitored the situation as well, vociferously protesting China's missile tests.

Not only has the military component of this crisis already escalated beyond the last one, but China has also escalated diplomatically and economically as well. A severe statement was released by China's Ministry of Foreign Affairs as Pelosi landed. The U.S. ambassador in Beijing, Nicholas Burns, was called into the Foreign Ministry to receive a formal *démarche* late that evening as well. Beijing also suspended or cancelled a series of planned bilateral exchanges. A set of well-crafted economic sanctions were levied against Taiwan, including several that appeared optimized to target the more assertive Democratic People's Party constituencies. Basic distributed denial-of-service attacks have shut down official and media web pages in Taiwan intermittently since Pelosi's visit. A polished white paper on the Taiwan issue was released, laying out the contemporary elements of China's policy. This coordinated activity is a significant achievement within the stove-piped Chinese political system, suggesting Beijing clearly planned well for the first stage of the crisis.

These are just the opening weeks. The historical record and current context suggest the situation is unlikely to settle quickly, even if Beijing wraps up its next round of military exercises in short order. In all of the previous Taiwan Strait crises, tensions and military activity ebbed and flowed. The first and third crises lasted approximately eight months, and the second over three.

International Factors

Today, international and domestic factors will interact to further complicate crisis management. All three primary actors will assess the messages they have sent and received and may conclude that additional signaling of resolve is necessary. China is trying to use military signals to dissuade the United States and Taiwan from continuing past policies. The United States and Taiwan are trying to show that they are not being deterred from continuing what they see to be rightful and consistent policies.

At first, China's actions were driven by the simple question of whether Pelosi would visit Taiwan or not. Going forward, Beijing will be responding to much more complicated questions. For instance, how "official" were Pelosi's activities in Taiwan? Does Japan's responses suggest Tokyo's policy is also shifting? If so, how much? In classic security dilemma fashion, Beijing may find that it has provoked more official engagement between Japan and Taiwan.

More fundamentally, Beijing sees Washington as moving away from its "One China Policy" and increasingly creating an official relationship with Taiwan. This undermines a core strategic interest for Beijing. Beginning with a cabinet level visit under the Trump administration and revision of rules for diplomatic engagement signed by then-Secretary of State Mike Pompeo, Beijing began to worry Washington was violating the commitments it made in establishing relations with the People's Republic of China during the Cold War. Public discussion of U.S. military forces in Taiwan, repeated off-the-cuff statements from President Biden, and changing language on official State Department web pages all, in Beijing's view, provide further evidence of this shift. Thus, an important goal for Beijing in the crisis is to deter further such salami slicing of the U.S. "One China Policy" more generally, as well as protesting the specific sliver that Pelosi's visit represents. This raises the stakes in the crisis and makes bringing it to a quick resolution less likely.

Furthermore, just as with economic sanctions leveled against Russia in response to its invasion of Ukraine, China's economic tools will take time to exact costs on the Taiwanese economy. There will be a strong logic for Beijing to retain these in place in the absence of any concession from Taipei. This too will keep tensions escalated.



America's national security apparatus will also be loath to let the appearance of Chinese military coercion go unchallenged. This is important for Washington's continued (if strategically ambiguous) support for Taiwan but also to help assure allies in the region, some of whom will be far more concerned with the Chinese exercises than U.S. domestic audiences. The mere presence of U.S. deployments discussed above will help on this front, but may, in themselves, be deemed insufficient. Indeed, the United States has already started talking about imminent Taiwan Strait transit missions and has deployed additional capital ships.

Another complication, from Beijing's side, is that the bureaucratic Chinese political system — not least the national security apparatus — remain sclerotic. This will make maintaining an integrated and coordinated response more challenging for Beijing as the pace of actions and reactions increase. Slow decision-making in Beijing characterized previous crises, such as the EP-3 incident in 2001 and the Belgrade embassy bombing of 1999. If the United States, Taiwan, and China intensify the tempo of military activity as the crises continues, such inertia will be dangerous.

Domestic Political Factors

Domestic factors in China, Taiwan, and the United States have also played a key role in creating this crisis and will continue to drive it. The Chinese Communist Party's reliance on nationalism in general, and specifically as related to Taiwan, will create pressure on the regime to live up to its self-proclaimed status as defender of China's unity. This will be particularly important from now through the fall when Xi Jinping, in a move unprecedented since the 1980s, plans to be reappointed to lead the party. There is some social media grumbling about Beijing's response inside China already. While censorship and repression can contribute to managing public opinion, Chinese leaders remain sensitive to it nonetheless.

In the United States, maintaining a confrontational approach to China now has bipartisan backing. As demonstrated by the recent passage of the CHIPS bill, treating China as a threat to be confronted is one of the few things that garners support from both sides of the aisle. This makes it harder for the United States to back down, just as it complicated internal discussions to dissuade Pelosi from going in the first place.

Finally, the Taiwanese people's deepening identification as Taiwanese rather than Chinese will make managing the cross-strait relationship even more difficult. This will color Taiwan's local electoral campaigns in the fall and in the more distant 2024 elections for president. It has already put the Democratic Progressive Party — which is committed to creating more "international space" apart from Beijing — in full control of most elements of Taiwan's government.

Risks of Escalation

While both strategic and political elements will exacerbate this crisis, it is not a prelude to a Chinese invasion. The timing is not suitable given China's political calendar, the Chinese military is too early in its modernization for an adventurous amphibious assault, and there is no sign of wholesale military mobilization. There is, as a result, no prospect of imminent U.S. preemption either. But despite this, there will be a lot of force posturing and militarized signals over the coming weeks and months. Inadvertent escalation is a concern, and the exacerbation of the existing security dilemma is guaranteed.

Inadvertent escalation can come in many forms. At the simplest level, human errors might occur. These are more likely during periods of high stress and long hours. Relatively junior officers have tremendous responsibilities in the U.S. military, and the Chinese system relies on rigid top-down command and control. Both raise risks in this regard. Misperceptions of military signals sent by opposing forces is also a major concern. One could imagine a variety of scenarios: Close monitoring, whether shadowing naval vessels or observing missile flights, will require high tempo operations. China engaged in a series of "unsafe" intercepts of U.S. and allied aircraft earlier this year. Those practices would presumably have been approved at high levels within the military and restraining them in a time of crisis will be challenging. Again, while not likely to lead directly to war, any escalation of tensions that is not deliberate serves no one's interest. In the longer term, we should expect a ratchet effect from this crisis. Beijing will certainly face future provocations that it will want to respond to. In those cases, China will view its response this time as a baseline and try to "do more."



This crisis will also inevitably exacerbate mutual suspicions in Washington and Beijing. There has already been a deterioration of relations between both sides, arguably beginning in 2008 and certainly accelerating since 2018. This crisis will deepen tensions and reify beliefs on both sides that the relationship is one of military competition.

Looking forward, there are steps all sides should take to minimize the damage and avoid conflict. The underlying military balance across the strait has changed, Chinese nationalism has taken on an ugly militarist tone, and Xi has implied some need for “progress” on the Taiwan issue. Clearly, the United States cannot unilaterally “solve” the crisis without abandoning an important regional partner. But provocations should serve strategic purposes. Selling man-portable surface-to-air missiles and potent coastal defense cruise missiles will certainly provoke the ire of Beijing, but their benefits in maintaining the cross-strait military balance will outweigh that. By contrast, flashy F-16 sales do little to defend Taiwan from China’s missile force. More realistic military policy and vastly increased budgets coupled with diplomatic efforts to reduce Beijing’s fear of abrupt pro-independence initiatives can help lower tensions. And, of course, if policymakers in Beijing are reading, they should also show greater restraint in place of the provocative attitude that has marked the last decade.

Whatever happens, the Fourth Taiwan Strait Crisis will be regarded as another important milestone in the deterioration of Sino-American relations. We have already crossed a number of worrisome thresholds, and the two main actors continue to posture for various strategic and domestic reasons. China, in particular, seeks to prevent a slow but steady shift in Taiwan’s status, while the United States seeks to reassure Taiwan and other allies. With careful statesmanship and a little luck, outright war can be avoided — but neither of these is ever guaranteed.

[The Fourth Taiwan Strait Crisis Is Just Starting - War on the Rocks](#)

[Return to Index](#)

How is China Trying to Redefine Power Balance in Taiwan Strait?

(DW 25 Aug 22)

Beijing's pledge to conduct "regular patrols" near Taiwan after large-scale military drills points to a worrisome and dangerous development, according to analysts.

After seven days of large-scale military exercises around Taiwan, the Chinese People's Liberation Army announced on Wednesday that the drills — held in response to a recent visit to the island by US House Speaker Nancy Pelosi — had concluded.

Beijing, however, pledged to continue "regular combat readiness patrols" in the area, raising the possibility of frequent Chinese military operations near the self-governed democratic island.

"I believe the Chinese are trying to change the status quo and create a new normal in the Taiwan Strait," said Bonnie Glaser, director of the Asia program at the German Marshall Fund.

"China decided they wanted to do something unprecedented and they wanted to demonstrate the development in their military capabilities and show their resolve," she added. "I'm concerned about the fact that they were explicitly demonstrating they can implement a blockade."

In a white paper published on Wednesday, China said it had zero tolerance for "separatist activities" in Taiwan.

While underlining its goal to achieve the "peaceful reunification" of Taiwan and China, Beijing also stressed that it "will not renounce the use of force, and we reserve the option of taking all necessary measures."

China also went on to threaten to use force against "interference by external forces or radical action by separatist elements."

US 'will not allow' isolation of Taiwan

The drills held in the wake of Pelosi's visit represent some of China's most provocative action toward Taiwan in decades.



During the exercises, the Eastern Theater command of the Chinese People's Liberation Army dispatched ships and fighter jets that regularly crossed the median line — an unofficial demarcation between China and Taiwan that the former does not recognize.

It also held anti-submarine drills, aimed at enhancing the ability of air and sea units to work together while hunting submarines.

The People's Liberation Army also test-fired 11 missiles into the surrounding seas, with four likely launched over Taiwan's capital, Taipei.

Taiwan has accused China of rehearsing possible invasion scenarios.

In Washington, Pelosi said on Wednesday that she was "very proud" of her delegation and believed China had used her visit as a "pretext" to launch its military exercises.

"We will not allow China to isolate Taiwan," she told reporters.

She also said the US could not allow Beijing to standardize a new level of pressure on Taiwan. "What we saw with China is that they were trying to establish sort of a new normal. And we just can't let that happen."

Beijing, however, retaliated by saying that Washington was the one that broke promises and violated China's sovereignty. "The US took the initiative to make provocations and then China responded with countermeasures, which are legitimate, justified, necessary and proper," Chinese Foreign Ministry Spokesperson Wang Wenbin said during Wednesday's daily press briefing.

'A new baseline for crisis protestation'

The ratcheting up of tensions between China and the US, and Beijing's pledge to conduct "regular patrols" near Taiwan, point to a worrisome and dangerous development, said Christopher Twomey, an expert on security affairs at the US **Naval Postgraduate School** in California.

"We could see the continued operation of Taiwanese forces and occasional transits of US forces in international waterways, and the more Chinese forces are routinely operating there, the more dangerous that is," he stressed.

"One of the real worries here is that the next time there is a political or diplomatic move that China feels that it needs to respond to, the Chinese may have to do even more next time. The idea that this being the new baseline for crisis protestation is also important to note."

While analysts have expressed concerns about China's aggressive military moves, the US said recent events had not changed its assessment that Beijing would not launch an invasion of Taiwan in the next two years.

Brian Hart, a fellow at the Center for Strategic and International Studies in the US, said Washington was trying to de-escalate the situation while not giving the impression that it was backing down in the face of Chinese pressure.

"The Biden administration also has to make sure that the US is not simply caving in to China's actions and the focus is on de-escalating while insisting that the US will continue to operate within international waters and within international law and continue to work with its allies and partners in the region," he said.

Hart stressed that Washington should continue its cooperation with Taipei in accordance with its longstanding official policy. "Instead of being loud and highly visible, do it in a way that's quieter while still making real substantial gains for Taiwan and US-Taiwan relations," he suggested.

The United States is Taiwan's primary military backer, selling Taipei much-needed weapons and defense tech. For decades, Washington has sold arms to the island under the Taiwan Relations Act, which allows for the supply of "defensive" weapons.

Since 2019, Taiwan has ordered at least \$17 billion (€16.65 billion) worth of US military equipment, according to Defense News. This includes an \$8 billion order of 66 F-16 fighter jets under former President Donald Trump, one of the largest single orders ever.

Preparing for the new status quo?

Twomey, from the US **Naval Postgraduate School**, said one of the outcomes that he hoped to see from China's recent military exercises was a more serious adoption of asymmetric or



"porcupine" capabilities and strategies by Taiwan, and less emphasis on expensive hardware such as fighter jets or large-scale naval platforms.

"They should focus more on enhancing the reserves and building up stockpiles of anti-ship cruise missiles that can be launched from coastal areas," he said.

To better prepare for the new status quo that Beijing is pushing for, Tzu-yun Su, an analyst at the Institute for National Defense and Security Research in Taiwan, said Taipei needed to show the rest of the world that it was not only relying on other countries to ensure its own security.

"Taiwan should also increase its defense budget, which Germany did earlier this year following the Russia-Ukraine war," he pointed out. "Additionally, Taiwan should prioritize military investment for ground-based air-defense missiles or ground-based anti-ship missiles, which form a more effective defense force quickly."

[How is China trying to redefine power balance in Taiwan Strait? | Asia | An in-depth look at news from across the continent | DW | 13.08.2022](#)

[Return to Index](#)

ALUMNI:

Salona Global Expands Management Team to Scale for Growth; Appoints New Chief Financial Officer for Salona, President for SDP Unit; Executes National Sales Distribution Agreement with Digitsole

(Yahoo! 22 Aug 22)

(Bolly Inside 22 Aug 22)

Salona Global Medical Device Corporation ("Salona Global," "SGMD," or the "Company") (TSXV:SGMD) announced that, in line with its rapid growth, it has appointed an experienced public company executive as Chief Financial Officer ("CFO") and promoted an operational executive as President of South Dakota Partners, Inc. ("SDP"), one of the Company's operating subsidiaries. Additionally, the Company has executed a national sales distribution agreement with Digitsole U.S Inc. ("Digitsole").

Dennis Nelson has been appointed CFO of Salona Global, effective August 29, 2022. Most recently he was Corporate Controller of Manscaped Holdings, LLC based in San Diego, California. Mr. Nelson was previously Principal Financial Officer of Alphatec Spine, Inc., a medical technology company trading on the NASDAQ. Mr. Nelson is a CPA with a BA in Business Economics from University of California, Santa Barbara.

Effective today, Mike Plunkett has been promoted to President of SDP, to replace Luke Faulstick, who was appointed CEO of Salona Global on July 18, 2022. Mr. Plunkett has served as a general manager for SDP since January 2019. Prior to that, Mr. Plunkett spent 25 years in the U.S. Navy rising to rank of Captain before moving into the private sector in multiple senior leadership roles including President of Alphatec Spine, Inc. Mr. Plunkett received a B.S. in Accounting from Saint John Fisher College, an M.S. in Financial Management from the **Naval Postgraduate School**, and an M.A. from the Naval War College.

"Salona Global is quickly becoming a larger and more complex enterprise and we are committed to recruiting experienced talent to our team as we drive rapid top line growth through acquisition and organic means," said Salona Global CEO Luke Faulstick. "We are fortunate to have Dennis and Mike in these key positions as we work towards closing and integrating the recently announced proposed acquisitions."

"We listed just last June with \$16 million in annualized sales," said Salona Global Executive Chairman Les Cross. "If we are successful in closing the next two transactions, we will have more than quadrupled our annualized sales, and must integrate multiple companies using varied financial systems."



Going forward, we must have a team that is sophisticated in filing financial documents with regulatory authorities in both Canada and the U.S., streamlining internal financial systems, and increasingly handling foreign sales transactions. As we prepare for our next stage of growth, we aim to be proactive by strengthening our management team. As we grow, we will continue to recruit talent to ensure we can take full advantage of our position in the market.”

Additional National Sales Distribution Agreement

Salona Global also announced it has further expanded its product line through a national distribution agreement with Digitsole, a leader in the digital health space based in France. Under the terms of the national distribution agreement, Salona Global’s subsidiary, Mio-Guard LLC (“Mio-Guard”), has gained the rights to distribute products from Digitsole in the US. Bringing together digital mobility biomarkers, biomechanical data, and clinical expertise to improve mobility and activity levels, Digitsole’s proprietary health technology was developed to monitor human movement digitally.

“We anticipate this Digitsole product line will drive revenue growth by expanding the products we offer to patients, athletic trainers, and physical therapists,” said Salona Global’s Executive Chairman Les Cross. “Strategically, along with the fine work that is already being done by our subsidiary Simbex, we are also positioning Salona as a leader in remote digital monitoring, mobility and health solutions.”

Salona Global is now offering Digitsole Pro, the human motion technology that helps healthcare practitioners improve their patient and business outcomes. This novel technology was developed by healthcare practitioners to measure biomechanical functions objectively, set baseline performance, and quantify the results of treatment. The system is portable and works using small sensors with a web interface and phone app. The Performance Rehab Module add-on product improves the technology by giving athletic trainers digital, quantified measurements of jump tests which can be administered in the field. The Digitsole products add to Mio-Guard’s existing product line, further expanding the offerings to athletic trainers and physical therapy clinics that assist in improving patient recovery outcomes, while also aiming to improve the financial performance of the offering clinic.

“We expect to generate increased revenues from these new products in the current quarter,” said Salona Global’s Chief Executive Officer Luke Faulstick.

[Salona Global Expands Management Team to Scale for Growth; Appoints New Chief Financial Officer for Salona, President for SDP Unit; Executes National Sales Distribution Agreement with Digitsole \(yahoo.com\)](#)

[Salona Global expands its management team to scale for growth; Appoints Salona's new finance director, president of the SDP department; It implements a domestic sales distribution agreement with Digitsole - Bollyinside - Today News](#)

[Return to Index](#)

Wisconsin Deputy Adjutant General For Air Completes Executive Leaders Program at Naval Postgraduate School

(Wisconsin National Guard 23 Aug 22) ... Sgt. 1st Class Katie Theusch

(Wisconsin Politics 23 Aug 22) ... Sgt. 1st Class Katie Theusch

Brig. Gen. David May, the Wisconsin National Guard’s deputy adjutant general for Air, completed the Executive Leaders program at the Naval Postgraduate School Center for Homeland Defense and Security (CHDS) on August 11th.

In his role, May serves as chief advisor to the adjutant general on all matters pertaining to Air National Guard programs, policies, operations, management and command and control of the Wisconsin Air National Guard. He also provides staff assistance guidance and direction concerning Air National Guard personnel, administration, training, recruiting and retention incentives and budgetary matters. May is responsible for more than 2,300 Wisconsin Air National Guard personnel serving in two flying wings and a Combat Readiness Training Center.



Throughout the hybrid program, May collaborated with homeland security officials from across the nation on current policy, strategy, and organizational design challenges.

“I’ve basically gotten recent immersion and exposure to the big issues of the day, whether it’s cybersecurity, logistics, COVID, dark sky events,” May said. “I’ve got a current education on where we’re at with those issues, as well as a lot of tools for leadership.”

The NPS-CHDS participants represent a snapshot of the homeland security enterprise, including professionals from the fields of emergency management, education, law enforcement, fire service, homeland security, public health, and city/county government.

“The network that you take forward is the powerful part,” May said. “This class has been around for 20 years. Not only are you networked with your own class, but you’re networked with the entire alumni of the entire program for the rest of your career.”

May added that the program exposed him to executive-level leadership at all levels – local, state, and federal. Collaboration and inclusion of the right people at all levels has led to successful partnerships and responses between the Wisconsin National Guard and domestic partner agencies, with the most notable being the Guard’s role in the state’s COVID-19 response.

“We’ve worked together enough over the years and planned together enough that we’re really ready to come together, so we need to keep doing that,” May said. “That inclusive approach, the collaborative approach is super powerful.”

He also learned the importance of quickly reassessing information and evolving throughout domestic operations responses.

“Do we spend energy criticizing ourselves? Or do we spend our energy adapting?” May said. “I would say adapt and move on. We really need to learn and relearn, acknowledge a mistake and move on, because that’s what the public that we serve needs from us. They need that continually evolving response.”

Located at the Naval Postgraduate School (NPS), CHDS is the nation’s homeland security educator. CHDS program participants develop critical thinking, leadership, and policy skills. CHDS is sponsored by the U.S. Department of Homeland Security (DHS), National Preparedness Directorate, within the Federal Emergency Management Agency (FEMA). For information, visit www.chds.us.

ABOUT NPS: The mission of the Naval Postgraduate School is to provide unique advanced education and research programs in order to increase the combat effectiveness of the U.S. and Allied armed forces as well as enhance the security of the United States. For information, visit www.nps.edu.

[Wisconsin’s Deputy Adjutant General for Air Completes Executive Leaders Program at Naval Postgraduate School – Wisconsin National Guard](#)

[Dept. of Military Affairs: Wisconsin’s Deputy Adjutant General for Air completes Executive Leaders Program at Naval Postgraduate School | WisPolitics.com](#)

[Return to Index](#)

USMSM Gets New Board Chair; Keane to Serve for Three Years

(Southern Maryland News 23 Aug 22) ... Caleb M. Soptelean

Jack Keane was recently named board chair of the University System of Maryland at Southern Maryland in California.

Keane, who was vice chair, will serve for three years beginning next year.

Keane was elected by the board at its quarterly meeting in July, a release from the university states.

Keane was raised in Holyoke, Mass., and graduated from Virginia Military Institute in 1980 with a degree in electrical engineering. Throughout his career as a naval officer, Keane served in many assignments around the world.

In 1993, he graduated from the **Naval Postgraduate School** in Monterey, Calif., with a degree in operations research. He retired in 1995 at the rank of lieutenant commander after serving at the Naval



Research Laboratory, where he flew research missions worldwide. Since his military career, Keane has been heavily involved in research and education.

He served as a member of the Johns Hopkins University Applied Physics Laboratory's principal professional staff, was branch supervisor of the Precision Strike Systems branch in the Force Projection Sector and was a member of Department of Defense's Simulation-Based Acquisition Joint Task Force.

Additionally, he was a member of the adjunct faculty of the JHU Whiting School of Engineering.

He is a past president and fellow of the Military Operations Research Society, having received its Wanner Award, the society's highest award for lifetime contributions to the field of Operations Research, in 2014.

In 2016, he was appointed to the Southern Maryland Higher Education Center's board of governors by Gov. Larry Hogan (R), and he was appointed to the board of advisors for USMSM in September 2019.

"I've lived in Charles County since 1993," he said. "In the nearly 29 years I've lived here, I've watched my neighbors come and go and, if they stayed, their children went away to college and never returned. Some went off to become engineers, mathematicians and analysts; others to become doctors, veterinarians and teachers. All that talent was leaving Southern Maryland. I thought this would be my opportunity to give back to Southern Maryland and demonstrate to the youth of the tri-county area that there are great opportunities right here at home."

"I'm incredibly excited about the new SMART building and the opportunities it has to bring in research dollars for robotics, un-crewed systems and autonomy – all of which will benefit not only the military, but law enforcement, first responders and the medical profession, to name a few," he said.

Keane's mission in his role as chair is to reach out to the tri-county area to expand the reputation of USMSM and the educational opportunities for underserved members of the community.

"We can do this by working with the local school systems, students and their parents to increase their awareness about affordable educational opportunities available right here at home," he said.

"Additionally, we need to expand the number of non-STEM programs, particularly in the agriculture and aquaculture areas. We also have a national shortage of teachers and veterinarians, and I believe USMSM can work to close those gaps for our community."

Joe Anderson, current chair of the board of advisors, is looking forward to transitioning the chair-elect.

"Since Jack joined our board three years ago, he's been integral to everything we've accomplished, and I think that's significant," Anderson said. "From our very successful merger with the University of Maryland to fighting for funds to build the SMART building, and then seeing the building constructed and opened for business, Jack was there every step of the way."

"Jack gets the big picture very well, but he also pays impeccable attention to the details of how we must get there," Anderson said. "He gets the job done. I can't think of a better person to chair the USMSM Board of Advisors, and I sincerely look forward to working under his leadership as we bring USMSM to great heights."

"Jack has a long history of supporting access to education in Southern Maryland," said Eileen Abel, USMSM's executive director. "We are grateful that he is stepping in to fill Joe's very big shoes."

[USMSM gets new board chair; Keane to serve for three years | Local News | somdnews.com](#)

[Return to Index](#)

