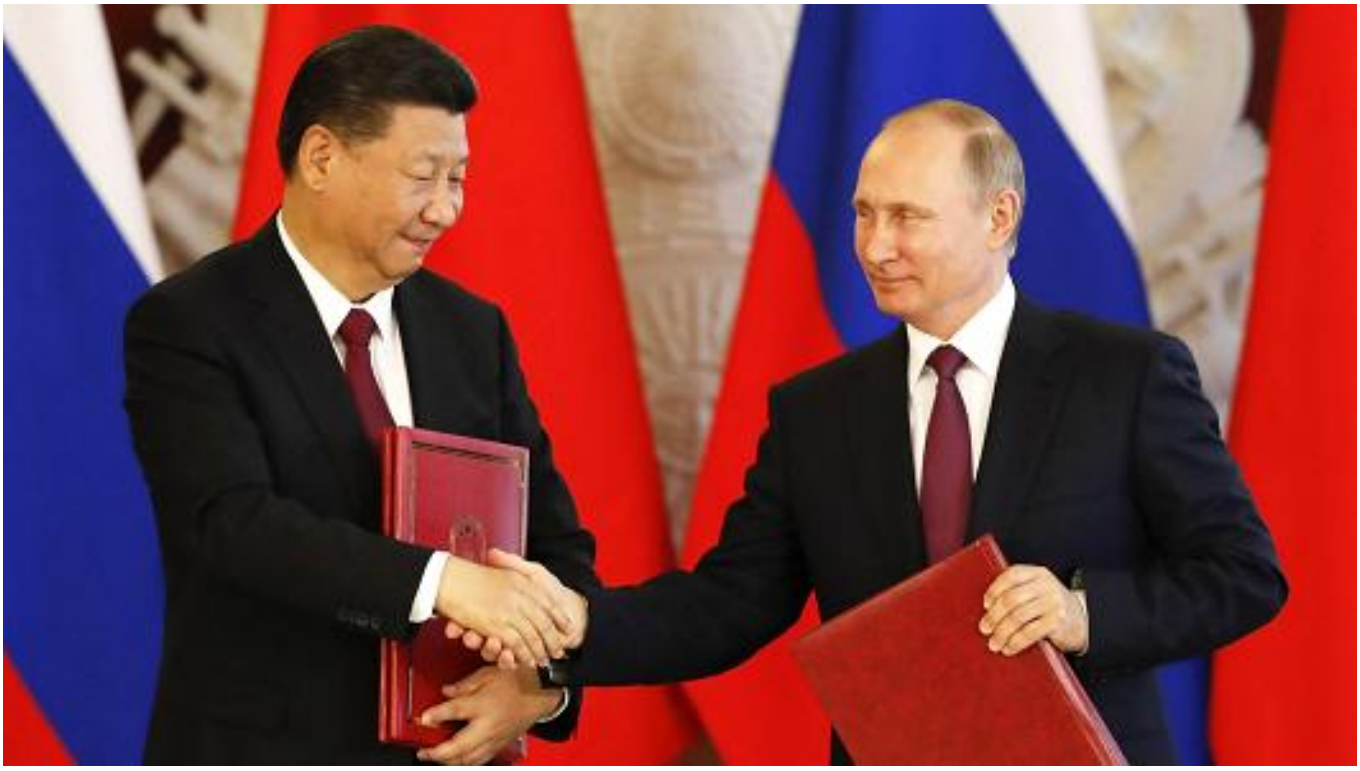
DEFENSE.info

Dealing with the Challenges of the 21st Century Authoritarian States



April 8, 2019

President Erdogan Resets Turkey's Course: The Role of the S-400 Issue

04/02/2019

By Robbin Laird

When I visited Turkey last year, it was clear in discussions in Istanbul with journalists and officials that President Erdogan was clearly on a path to break with the traditions of Ataturk and the secular state.

In a period where the global impact of the various strands of Islam are clearly providing significant global impact, the President of Turkey has focused on emphasizing the Islamic side of Turkey, not its secular tradition and its role as a leader in the Middle East shaping a more effective democratic path forward in a troubled region.

In place of Ataturk's vision, we have the Erdogan vision of a partial restoration of the Ottoman Empire with an expanded role of Turkey as a leading Islamic state operating in Africa and the Middle East. He has also overseen the significant economic decline of Turkey which means that the focus on the restoration of Turkish "glory" is not going to be funded by a dynamic Turkish economy closely integrated with the West.

In a critical but insightful article by Alon Ben-Meir on Erdogan , the author hihglights the psedo-Ottoaman approach being followed by the President.

"With little or no opposition at home, Erdogan moved to promote his Ottoman penchant to establish military bases in Qatar and Somalia, and military ties with Tunisia.

Now he is scheming to build another military installation on the strategically located Sudanese Island of Suakin. Erdogan intends to utilize the island as a military outpost, as it had been during the Ottoman era. Egypt and Saudi Arabia believe that Erdogan's military adventure will upset the regional balance of power, which is the recipe for instability and incessant violence."

With regard to military policy, a key part of his effort is to build out the autonomy of Turkish industry and to do so at the expense of the quality of his forces. He used the "coup" to rip apart the Turkish Air Force and create a much less effective military force. In my discussions with journalists in Istanbul, the drive for arms independence was highlighted as a key issue and there was clear concern that collaborative programs with the West, such as the F-35 would unravel.

There was a discussion of the challenges the West played with regard to Erdogan because arms programs have been a key means whereby effective working relationships with Turkey have been maintained over the years. Indeed, one could note that without the collaborative working relationships of the professional military and collaborative defense industrial working relationships, NATO itself would be much less real and much less effective.

But Erdogan is acting is if his membership in NATO is a birthright which allows him significant room for maneuver to expand South and East. The time is fast approaching when he needs to learn that he has significantly less room for maneuver if he continues to stab the West in the back.

An excellent example of how Erdogan is operating is his recent exploitation of the horrific slaying of Muslims in New Zealand. During his current electoral campaign, he thought it acceptable to threaten the ANZAC community if they did not do whatever he thought was appropriate.

Ataturk was a brilliant Turkish military leader who defeated the allies in World War I when the attack was made on Turkey; he was respected because of his combat brilliance and because he went on to

make Turkey a great nation. Erdogan who has no such pedigree seems to think that standing on the dead bodies of World War I soldiers and threatening their descendants will have no consequences.

He is playing fire as well with his nation's security by clearly putting his country on the path to be booted out of the F-35 program.

Although the French defense minister recently commented that Germany could not buy the F-35 and still be part of Article V, what she missed is that for several key NATO partners, the F-35 is a key building block of deterrence of Russia.

These partners will not welcome a Turkey F-35 partner willing to compromise the technology by now turning to Russia for arms. It is not about equivalence; it is about commitment.

The Turks are part of the F-16 European community and as such joined F-35

With the strategic shift from the land wars to dealing with the Russians and other competitors, and the slow roll involvement in the land wars, the F-35 has come at a time when the US and allies are focusing on high end conflict

The F-35 is central to that but because it is not a classic fighter but a flying combat system we are leveraging it to connect to other warfighting assets like Aegis

The connected warfare piece is central to the F-35 And given what the Israelis have already demonstrated against the Russians in Syria, we clearly are not interested in an F-35 partner playing with the S-400 and seeking in any way to combine those capabilities on their own.

The Turks provide some key elements as part of the F-35 global enterprise for the airplane but we can of course shift from Turkey to suppliers elsewhere

But the problem is that Turkey seems to be throwing its fate in with the authoritarian powers — China and Russia — which is not a good sign and certainly will lead the US to deny them F-35s

How do the liberal democracies prevail in dealing with their authoritarian competitors?

04/27/2018

By Robbin Laird

he challenge posed by competitors such as modern China and Russia is both significant and different from what we have seen both in the recent past and during the Cold War.

We are in a fundamentally different historical era. Russia is not the Soviet Union. And China is not Mao's PLA. There are lessons learned from the past and domain knowledge, which can be leveraged in the migration in back to the future to harvest the best but leave the rest, such knowledge is to be leveraged not slavishly copied.

We must also try and learn what we don't know.

Effective military organizations around the globe respect what Secretary Rumsfeld once sagely focused on "the unknown unknowns"

This problem was put very clearly in a recent interview with the Royal Australian Air Force head of their Air Warfare Centre , which is totally focused on joint warfare as the driver for change.

Throughout the interview, he was very clear on the importance of breaking out of legacy patterns and thinking and finding ways to train for the future fight with the force you are crafting and respect what one doesn't know.

"Our senior leadership, including myself, has never grown up in the combat environment which is now evolving rapidly. We need to unlearn as well as learn to shape an effective way ahead."

"The change is to effectively shape a future force structure based on where you need to go, rather than what you have inherited?

I would add that this is not just true for the military but for civilian strategists, policymakers and politicians.

What is the nature of conflict we are facing posed by peer competitors?

How do compete more effectively?

How do we protect our way of life?

How do we prevail in the conflict with the illiberal societies?

As the Chief of the Australian Navy put it bluntly: "We are not looking at conflict between platforms, or segments of the military against adversaries.

"It is a fundamental test of conflicting approaches to conflict and to warfare."

This comment put the challenge where it needs to be, namely, the demand set is broadening as the range of tools for conflict also increase; and the potential impact from miscalculations are ramping up with the consequences for prolonged armed conflict among peer competitors.

What is clear now is that a new phase is beginning which requires clear-headed analysis and preparation of tools sets, which can effectively protect the ways of life and strategic interests of the liberal democracies.

The tectonic plates are shifting and the liberal democracies need to think carefully about the prospects and consequences of these profound changes between (and within) nations, and how best to respond to this new world order (or disorder).

Security threats have unleashed national reactions with various nations seeking to rebalance their position in the global order, and seeking to work with clusters of either like-minded states, or with states capable of providing key needs.

It is not exactly the return of nationalism, for that has not been absent in any case, but is clearly the return of security and defense concerns as a priority, and these concerns are always led by states seeking allies, partners or friends, or "the enemy of my enemy is my friend" types of partners.

Put in other words, the return of hard power combined with various other tool sets is being exercised to try to reshape the global situation to the advantage of the illiberal powers.

The nature of the threat facing the liberal democracies was well put in last years Finnish Defence White Paper: "The timeline for early warning is shorter; the threshold for the use of force is lower."

What is unfolding is that capabilities traditionally associated with high-end warfare are being drawn upon for lower threshold conflicts, designed to achieve political effect without firing a shot.

Higher end capabilities being developed by China are Russia are becoming tools to achieve political-military objectives throughout the diplomatic engagement spectrum.

This means that not only do the liberal democracies need to shape more effective higher end capabilities but they need to learn how to use force packages which are making up a higher end, higher tempo or higher intensity capability as part of a range of both military operations but proactive engagement to shape peer adversary behavior.

The non-liberal powers are clearly leveraging new military capabilities to support their global diplomacy to try to get outcomes and advantages that enhance their position and interests.

The systems there are building and deploying are clearly recognized by the Western militaries as requiring a response; less recognized is how the spectrum of conflict is shifting in terms of using higher end capabilities for normal diplomatic gains.

To be blunt, the distinction which Joe Nye suggested between hard and soft power is being changed by the military revolution. 21st Century military systems are really about hard power redesigned to be more useful in supporting political objectives, which if one wants to call that soft power then I am not sure the distinction has meaning.

Should America Tackle All Authoritarian Governments?

03/02/2019

By Hunter DeRensis

This past February, California Democrat Adam Schiff, who is chairman of the House Intelligence Committee, wrote an open letter to his Republican colleagues in the Washington Post. In it, he stated, “The time for silent disagreement is over. You must speak out.”

Since then, Schiff has moved steadily not only to investigate the Trump administration’s ties with Russia, but also to launch a broader crusade against authoritarian regimes abroad, defining their very existence as a threat to American democracy.

By his logic, America should embark upon a permanent campaign against autocracy, anywhere and everywhere it might appear.

This past Tuesday marked the first hearing of the House Intelligence Committee in the new congressional term, now under Democratic control. While there is a laundry list of topics the committee could have chosen to begin with, Schiff was adamant about tackling what he refers to as “an issue that may surpass them all in importance, and yet underlies each: the rise of authoritarianism and the threat to liberal democracy around the world.”

His arguments were prefigured in an essay that he wrote earlier in the week for the Atlantic in which he stated:

“Across the globe, democracies are mired in an ugly brand of populism often directed against ‘the other,’ and are displaying a troubling receptivity to autocracy as an alternative model of governance. If these trends continue, it will be a tragedy for humankind and a disaster for our national security.”

The language is apocalyptic, the claims sweeping.

What amounts to Schiff’s personal mandate for leadership inadvertently underscores that much of the Washington foreign policy establishment continues to cling to the verities of the Cold War….

In theory, this might sound like a good idea, but in practice it raises a host of questions—none of which were really addressed by the speakers that testified to the committee.

America has long practiced a selective morality about what regimes it supports. Is Saudi Arabia less heinous than Iran?

At what point does a regime qualify for autocratic?

Should the so-called "illiberal democracies" such as Hungary be banned from polite society?

And so on.

For the rest of the article, see the following:

https://nationalinterest.org/feature/should-america-tackle-all-authoritarian-governments-45867

China's "Buy In" Strategy for Maritime Operations in the Pacific: Putting It into a Strategic Maritime Context

03/30/2019

By Robbin Laird

China has expanded its maritime reach as it modernizes its navy and air force. And has done so through a "buy in strategy" but one that is challenged as well with its approach to "gray zone operations" in the region as well.

In a recent article by Leland Lazarus andJohn Brunetti, the "buy in" approach is discussed.

China continues to roil Asian neighbors over claims in the East and South China Seas. However, China has also been cooperating with neighbors to establish codes of conduct to reduce conflict in the maritime arena. For years, China and the Association of Southeast Asian Nations (ASEAN) negotiated maritime codes of conduct.

More recently, China hosted the signing of the Code for Unplanned Encounters at Sea in 2014. In February 2018, China and ASEAN held a two day tabletop exercise in Singapore, where defense ministers from eleven countries planned responses to potential oil tanker fires, search and rescue evacuations, and naval assistance to merchant vessels and civilian ships. And in October last year China and ASEAN organized an inaugural five-day maritime field training exercise.

More than one thousand personnel—deployed on eight ships from Brunei, China, the Philippines, Singapore, Thailand, and Vietnam—conducted exercise drills in the Ma Xie naval base in Zhanjiang, China.

According to exercise co-director Colonel Lim Yu Chuan of Singapore, the exercise drills "enabled us to strengthen interoperability and more importantly, build trust and confidence for our navies to work with one another in responding to maritime incidents at sea." Despite the maritime claim tensions, regional powers are beginning to buy into a cooperative relationship with China.

A second element of the "buy in strategy," according to the authors is the Chinese maritime reach into the Middle East and Africa, where the Chinese Navy has assisted in counter-piracy operations

PLAN has escorted more than 6,400 Chinese and foreign ships, and prevented about 3,000 suspected pirate boats from launching attacks in the Gulf of Aden. China's maritime initiative is also evident in the South Pacific. The Peace Ark,

China's ten-thousand-ton medical ship, provided free medical treatment to twenty thousand patients in Papua New Guinea, Vanuatu, Fiji, and Tonga. Such exercises show China's transition into a blue water navy, and dovetails nicely with China's narrative of being a peaceful, cooperative neighbor, and not a competitor to be feared.

The third element of the "buy in strategy" is in the area of expanding port ownership as part of its global silk road strategy.

Over the past decade, China has helped finance at least thirty-five ports around the world. One flagship project is the Gwadar port in Pakistan. Part of the $62 billion China-Pakistan Economic Corridor (CPEC) initiative, China is helping Pakistan update the Gwadar port

A final element of what the author's call a "buy-in strategy" is the Chinese shipbuilding industry.

Today, China's ship construction dominates the world market. CSSC's Jiangnan Shipyard and Hudong-Zhonghua Shipbuilding recently began building the world's largest container ships. These ships are a marvel of size and technology using liquid natural gas to deliver goods the world over. China is also willing to sell existing ships to allies; for instance, China just agreed to sell its aircraft carrier Liaoning to Pakistan. For allies, seeing such transactions certainly sweetens the deal of working with China.

We could put this differently and see what the author's are calling a "buy in strategy" as key elements of an overall maritime influence strategy designed to expand the power of the authoritarian state at the expense of the liberal democratic order.

This is clearly a global influence strategy in which the "soft power" approach is underwritten by the willingness to use force to support its impact and influence.

The "gray zone" approach being followed by China is a constant reminder to states that China has presence and is willing it to reshape the maritime order to its preferences.

A recent book edited by Andrew S. Erickson and Ryan D. Martinson on Chinese maritime operations looks at "gray zone" operations being conducted by the Chinese.

The book identifies and discusses in detail "gray zone" operations, namely, operations short of the use of lethal force but empowered by a well worked out chain of maritime power elements up to and including the presence of combat forces.

The goal is to reshape the external environment in ways favorable without the need to engage in kinetic operations. In the hybrid war concept, lethal operations are the supporting not the tip of the spear element to achieve what the state actor is hoping to achieve tactically or strategically.

The book argues that this is a phase short of what the Russians have done which has been labelled hybrid warfare.

But from my point of view both gray zone ops and hybrid war ops are part of a broader strategic reality, namely, the nature of crisis management facing the liberal democracies competing with the authoritarian states in a peer-to-peer competition.

And I would subsume the "buy-in strategy" as part of the broader capabilities which can indeed shape how crosses can be avoided, influenced or dominated by the Chinese. In the US, the kind of activity which the Merchant Marine or the Coast Guard does has NEVER been incorporated into the broader influence strategy. For the Chinese, these capabilities, including economic activities have been.

The separation of activities so important to the success of capitalism, is ignored by the Chinese as an authoritarian state and instead works to integrate the spectrum of activities from peace to war in a quite different manner.

The challenge can be put bluntly — deterrence has been designed on the Western side with large scale engagement of enemy forces in mind.

What if deterrence in this sense is the necessary but not sufficient capability to constrain the actions of the authoritarians?

What if you can deter from full scale war, but by so doing not be able to control what your adversary is doing in terms of expanding his global reach and reshaping the strategic environment to his benefit?

What if you have organized yourself for deterrence but not effective crisis management?

The gray zone concept in my view is subsumed in this broader strategic shift and challenge.

There is also a key question whether gray zone operations is the strategic focus or really a phase on the way to engaging in kinetic operations as part of the way ahead.

What if the US and its key allies are not willing or able to respond and the Chinese expand their appraoch over time?

We can not assume that as Chinese look at the world or read RAND studies that they will not believe that actually striking a US or allied warship might not be a useful part of their evolving appraoch to crisis management.

From this point of view the discussions of the book could be seen as a historic look at a phase of Chinese maritime power and the evolving approach to strategic engagement in the region and beyond.

I would note that the focus in the book is on the US Navy and its responses.

Having worked with the USCG for years, I found the resource neglect of the service and the strategic decision to stick them into the Department of Homeland security as significant strategic failures on the part of the US.

First, the engagement in the Middle East has stolen resources from many security and non-security accounts, among them the USCG.

And then the focus on the return of Great Power politics, although admirable must focus on the nature of who these competitors actually are and how they operate.

How do we constrain Chine, and not just deter it?

Many years ago when I started a series on Pacific defense for the then AOL Defense, now Breaking Defense, I actually started with the significance of the USCG and why they were a foundational element for the kind of "constrainment" as well as deterrent strategy we needed to shape.

That series led eventually to our co-authored book on Pacific strategy which again started with the "constrainment" challenge not just the deterrence one.

What I had not realized was that it is the broader challenge which the authoritarian states were generating for crisis management against the liberal democracies which was in play.

And that this was the core strategic shift from the land wars.

This book simply validates how important the missing USCG National Security and Offshore Patrol vessel hulls and trained personnel are.

Instead, the US focused on Littoral Combat Ships which made no sense.

The white hulls are crucial to a "constrainment strategy", and the expansion of the Chinese Coast Guard in the region has been central to the gray zone operations discussed in the book.

Or let me be blunt: What the Chinese have done should not be a strategic surprise or a black swan.

It is simply something for which we did not prepare nor resource.

In effect, the "buy in strategy" when combined with the Chinese approach to "gray zone operations" and its expanded capability to fight at the high end really work together to underscore that China is not a liberal power wishing to reinforce current rules of the maritime order.

Rather, they a modern authoritarian power seeking to work with its allies to reshape the global order in a more favorable manner to themselves.

In the second edition of their highly regarded book on Chinese maritime power, Toshi Yoshihira and James R. Holems, what one Chinese analyst has called the "cabbage strategy."

Zhang Zhaozhong—a retired rear admiral, NDU professor, well-known television personality, and prolific author of nationalistic navalist books for popular consumption—explain(s) how a cabbage strategy works. The strategy, Zhang says, can be encapsulated in "just one word, which is squeezing."

His explanation is worth quoting at length: "For every measure there is a countermeasure.…If you send fishing vessels to resupply, then we will use fishing vessels to keep them out; if your coast guard sends supplies, then we will send marine surveillance to keep them out. If your Philippine Navy ships hurry over, we will use naval vessels to keep them out. There is nothing to be afraid of, and we must stick it out to the end. The cabbage strategy of which I have spoken many times is to surround them layer by layer, and make them unable to enter [Second Thomas Shoal].48 (Our emphasis)."[1]

A key disconnect between Western navies and the Chinese over the past few years has been a clear focus by Western navies on maritime missions to support the global trade order whereas the Chinese have been focused on conflict at sea as well as global trade order missions.

China's approach poses problems from a cultural standpoint as well. In the sense that "Mahanian" connotes girding for fleet battles and "post-Mahanian" means policing the sea or projecting power ashore, China is comfortable using post-Mahanian means for Mahanian ends.

A fishing trawler or coast guard cutter represents an implement of power politics as surely as a warplane or a hulking destroyer.

For their part, U.S. naval officers find it hard to deal with white-hulled China Coast Guard cutters or maritime enforcement vessels trying to cement command of Chinese-claimed waters. Countermeasures for maritime militia embedded within the fishing fleet and working in conjunction with law enforcement ships are still harder to come by.[2]

The authors note that this is changing as the US Navy begins to refocus on conflict at sea as a core mission and is modifying its combat assets to be more capable of so doing.

The authors conclude their book by looking at ways the US might more effectively counter the Chinese approach and to enhance core combat capabilities.

And it is China's mounting resistance to the U.S.-led system of trade and commerce, which has nourished the regional order for more than seven decades, that makes the rise of Chinese sea power so worrisome.

Policy makers, then, must resist the temptation to focus narrowly on the material or operational dimensions of Chinese anti-access.

These are important beyond a doubt. But statesmen must recognize that China's ascent and its accompanying dream pose an all-encompassing challenge to the United States and the long peace over which it has presided in Asia.[3]

I would add that a major aspect of working mid-term and long-term responses to the Chinese and to shape ways to constrain them is clearly how the US works with core Asian allies.

The military-technical aspects of so doing are important but so are the political-military as well as diplomatic.

But bluntly, how Japan, Australia, the South Koreans and others work together with the US in shaping the next phase of the liberal order is a crucial concomitant of the refocus on what the authors refer to as the "Mahanian" focus which connotes girding for fleet battles and "post-Mahanian or policing the sea or projecting power ashore.

The authors deal with the allied dimension in the context of how the Chinese see the general challenge facing them with regard to their core security challenges.

Geography colors how Chinese strategists appraise threats. The Korean half-island and the Japanese archipelago converge on key bodies of water while forming straits near China's political and economic centers.

Whether the U.S.–Japan–South Korea alignment can ever become a coherent strategic unit is dubious at best in light of the two Asian allies' turbulent past.

Nevertheless, Chinese observers find it unsettling that two U.S. allies boasting advanced economies and modern armed forces stand athwart sealanes essential to China's security and economic health.

Sowing disunion among the allies would partly ameliorate this dilemma—and thus represents a strategic imperative for Beijing.[4]

Indeed, from my perspective working the technology and working the US and allied concepts of operations along with reshaping how the alliance will work in the presence of persistent Chinese efforts to change that Alliance is at the heart of the challenge.

For US policy makers, rebuilding the US Navy is a necessary but not sufficient condition; working more effective allied relationships to constrain and channel the Chinese is crucial as well.

In short, at the heart of the Chinese transition with regard to seapower is the shift from benefiting from and leveraging the global liberal system which has been underwritten by the US Navy to shaping their own capabilities to defend their interests, operate globally and to provided extended defense of their crucial port regions, where significant population and economic capabilities are located.

And it is not just about the numbers and capability of their gray hulls; it is about the sweep from a "buy in strategy" to "gray zone operations" to "economic presence" in the global maritime system and shaping higher-end capabilities which could come into play as crises occur and need to be managed.

Note: This is what I wrote in my piece on AOL Defense in the second piece in my Pacific series and published on August 14, 2012:

As Vice Admiral Manson Brown, the recently departed Coat Guard Pacific commander, underscored in an interview last year:

"Many people believe that we need to be a coastal coast guard, focused on the ports, waterways, and coastal environment.

"But the reality is that because our national interests extend well beyond our shore, whether it's our vessels, or our mariners, or our possessions and our territories, we need to have presence well beyond our shores to influence good outcomes.

"As the Pacific Area Commander, I'm also the USCG Pacific Fleet Commander. That's a powerful synergy. I'm responsible for the close-in game, and I'm responsible for the away game. Now the away game has some tangible authorities and capabilities, such as fisheries enforcement and search and rescue presence," he said.

At the heart of a strategic rethink in building a U.S. Pacific maritime security strategy is coming to terms with the differences between these two domains, the security and military. The security domain is based on multiple-sum actions;

military activity is by its very nature rooted in unilateral action. If one starts with the military side of the equation and then defines the characteristics of a maritime security equation the formula is skewed towards unilateral action against multiple-sum activity.

But there is another aspect of change as well. Increasingly, the United States is rethinking its overall defense policy. A shift is underway toward preparing its forces for global operations for conventional engagement in flexible conditions.

Conventional engagement is built on a sliding scale from insertion of forces to achieve political effect to the use of high intensity sledgehammer capabilities. Policymakers and specialists alike increasingly question the utility of high-tech, high-intensity warfare capabilities for most conventional engagement missions.

In parallel to the relationship between those two domains is the relationship between the Coast Guard and the Navy, rooted in a sliding scale on levels of violence. This needs to be replaced by a new look, which emphasizes the intersection between security operations and conventional engagement, with high-intensity capabilities as an escalatory tool.

To protect the littorals of the United States is a foundational element for Pacific defense, and allows the U.S. to focus on multiple sum outcomes to enhance defense and security, but at the same time it lays a solid foundation for moving deeper into the Pacific for military or extended security operations when needed.

A reflection of such an approach is the North Pacific Coast Guard Forum. Again one must remember the central place the Great Circle Route plays in trans-Pacific shipping and the immensity of the Pacific. Given these conditions, the Coast Guard has participated in a collaborative security effort in the North Pacific designed to enhance littoral protection of the United States.

Among the key participants are the Canadians, Russians, the Japanese, the South Koreans and the Chinese.

Admiral Day, an active participant in the forum during his tenure, notes that members have participated in numerous exercises and several joint operations.

But for the United States to play a more effective role in defending its own littorals and to be more effective in the kind of multi-national collaboration which building Pacific security and providing a solid foundation for littoral defense, a key element are presence assets.

"And it's presence, in a competitive sense, because if we are not there, someone else will be there, whether it's the illegal fishers or whether it's Chinese influence in the region," said Vice Adm. Manson Brown. "We need to be very concerned about the balance of power in the neighborhood.

If you look at some of the other players that are operating in the neighborhood there is clearly an active power game going on. To keep the US presence relevant, the Coast Guard's National Security Cutters are a core asset.

The inability to fund these and the putting in limbo of the smaller cutters, the so-called OPCs, or Offshore Patrol Cutters, underscores a central question: without effective littoral presence (for U.S. shores) how does one do security and defense in the Pacific?

The size and immensity of the Pacific means you operate with what you have; you do not have shore infrastructure easily at hand to support a ship. Ships need to be big enough to have onboard provisions and fuel, as well as aviation assets to operate over time and distance.

In short, providing for littoral defense and security on the shores of the United States requires a reaffirmation of the Coast Guard's Title X role and ending the logjam of funding support for the cutter fleet and the service's aviation assets which enable that fleet to have range and reach.

The Return of Direct Defense in Europe: The Challenge to the Infrastructures of the Liberal Democratic Societies

04/06/2019

By Robbin Laird

Russia and China as 21st century authoritarian powers are challenging the liberal democracies in both classic military terms as well as in less classic ways.

The Russians with their approach to hybrid warfare and the Chinese with their evolving operational approaches in the "gray zone" are crafting innovative approaches to enhance their objectives short of significant engagements with peer competitors.

They are working to push the "red line" further down the spectrum of conflict and shaping a wider range of operational space within which their forces and capabilities can achieve desire objectives.

Another key area in which they are operating is with the direct engagement of their peer competitors is through expanded control or influence within the infrastructures of the economies and societies of those competitors.

The Finnish Perspective

The Finns have focused squarely on ways to enhance their capability to resist incursions from the Russians and to work towards expanded ways to enhance democratic military capabilities. They prioritize security of supply and have maintained military inscription system to prepare to mobilize in a crisis as well.

The Finns recognize that this is not enough given the nature of their 21st century competitor. They have established a new Centre to deal with the challenge of not just new ways of conducting influence operations but against European infrastructure as well. And they have done so in a manner which underscores that a purely national solution is not enough and requires a broader European Union response as well.

The Government of Finland has stood up a new Centre designed in part to shape better understanding which can in turn help the member states develop the tool sets for better crisis management.

This is how the Finnish government put it with regard to the new center in its press release dated October 1, 2017.

The European Centre of Excellence for Countering Hybrid Threats has reached initial operational capability on 1 September 2017. The Act on the European Centre of Excellence for Countering Hybrid Threats entered into force on 1 July 2017, following which Matti Saarelainen, Doctor of Social Science, was appointed Director of the Centre. The Centre has now acquired premises in Helsinki, established a secretariat consisting of seven experts and made the operational plans for this year.

"Hybrid threats have become a permanent part of the Finnish and European security environment, and the establishment of the Centre responds well to this current challenge.

Since early July, rapid progress has been made to allow the Centre to begin its operations. The Steering Board will be briefed on the progress at its meeting next week," says Jori Arvonen, Chair of the Steering Board of the Centre.

The Centre will launch its activities at a high-level seminar to be held in Helsinki on 6 September. The seminar will bring together representatives of the 12 participating countries, the EU and NATO. Approximately 100 participants will take part in the seminar. The Centre's communication channel (www.hybridcoe.fi) will also be opened at the seminar. Minister for Foreign Affairs Timo Soini and Minister of the Interior Paula Risikko will speak at the seminar as representatives of the host country. The official inauguration of the Centre will be held on 2 October.

The Centre is faced with many expectations or images. For example, the Centre is not an ´operational centre for anti-hybrid warfare´ or a ´cyber bomb disposal unit´. Instead, its aim is to contribute to a better understanding of hybrid influencing by state and non-state actors and how to counter hybrid threats. The Centre has three key roles, according to the Director of the Centre.

"First of all, the Centre is a centre of excellence which promotes the countering of hybrid threats at strategic level through research and training, for example. Secondly, the Centre aims to create multinational networks of experts in comprehensive security. These networks can, for instance, relate to situation awareness activities. Thirdly, the Centre serves as a platform for cooperation between the EU and NATO in evaluating societies' vulnerabilities and enhancing resilience," says Director Matti Saarelainen.

The EU and NATO take an active part in the Centre's Steering Board meetings and other activities. As a signal of the EU and NATO's commitment to cooperation, Julian King, EU Commissioner for the Security Union, and Arndt Freytag von Loringhoven, NATO Assistant Secretary General for Intelligence and Security, will participate in the high-level seminar on 6 September.

Currently, the 12 participating countries to the Centre are Estonia, Finland, France, Germany, Latvia, Lithuania, Norway, Poland, Spain, Sweden, the United Kingdom and the United States. EU and NATO countries have the possibility of joining as participant countries.

http://valtioneuvosto.fi/en/article/-/asset_publisher/1410869/eurooppalaisen-hybridiosaamiskeskuksen-toiminta-kaynnistyy-helsingissa

During a 2018 visit to the Centre, we interviewed Päivi Tampere, Head of Communications for the Centre, and with Juha Mustonen, Director of International Relations and discussed the approach of the new Centre to the authoritarian states.

The Centre is based on a 21st century model whereby a small staff operates a focal point to organize working groups, activities and networks among the member governments and flows through that activity to publications and white papers for the working groups.

As Tampere put it: "The approach has been to establish in Helsinki to have a rather small secretariat whose role is to coordinate and ask the right questions, and organize the work.

"We have 13 member states currently. EU member states or NATO allies can be members of our Centre."

"We have established three core networks to address three key areas of interest.

"The first is hybrid-influencing led by UK;

"The second community of interest headed by a Finn which is addressing "vulnerabilities and resiliencies."

"And we are looking at a broad set of issues, such as the ability of adversaries to buy property next to Western military bases, issues such as legal resilience, maritime security, energy questions and a wide variety of activities which allow adversaries to more effectively compete in hybrid influencing."

"The third COI called Strategy and Defense is led by Germany.

"In each network, we have experts who are working the challenges practically and we are tapping these networks to share best practices what has worked and what hasn't worked in countering hybrid threats.

“The Centre also organizes targeted trainings and exercises to practitioners.

“All the activities aim at building participating states’ capacity to counter hybrid threats.

“The aim of the Centre’s research pool is to share insight to hybrid threats and make our public outreach publications to improve awareness of the hybrid challenge.”

With Juha Mustonen, who came from the Finnish Ministry of Foreign Affairs to his current position, we discussed the challenges and the way ahead for the Centre.

“Influencing has always been a continuum first with peaceful means and then if needed with military means.

“Blurring the line between peace time influencing and war time influencing on a target country is at core of the hybrid threats challenge.

“A state can even cross the threshold of warfare but if it does not cross the threshold of attribution, there will be no military response at least if action is not attributed to that particular state.

“Indeed, the detection and attribution issue is a key one in shaping a response to hybrid threat.”

And with the kind of non-liberal states we are talking about, and with their expanded presence in our societies, they gain significant understanding and influence within our societies so they are working within our systems almost like interest groups, but with a focus on information war as well.

Mustonen: Adversaries can amplify vulnerabilities by buying land, doing investments, making these kinds of economic interdependencies.

“They can be in dialogue with our citizens or groups of our citizens, for example, to fostering anti-immigrant sentiments and exploiting them to have greater access to certain groups inside the European societies.

“For example, the narratives of some European far right groupings have become quite close to some adversaries’ narratives.”

Question: But your focus is not only on the use of domestic influence but mixing this with kinetic power as well to shape Western positions and opinion as well, isn’t it?

Mustonen: Adversaries are using many instruments of power. One may identify a demonstration affect from the limited use of military power and then by demonstrating our vulnerabilities a trial of a psychological affect within Western societies to shape policies more favorable to their interests.

“If you are using many instruments of power, below the threshold of warfare, their synergetic effect can cause your bigger gain in your target societies, and this is the dark side of comprehensive approach.”

“The challenge is to understand the thresholds of influence and the approaches.

“What is legitimate and what is not?

“And how do we counter punch against the use of hybrid influencing by Non-Western adversaries?

“How can we prevent our adversaries from exploiting democratic fractures and vulnerabilities, to enhance their own power positions?

“How do we do so without losing our credibility as governments in front of our own people?”

Clearly, a key opportunity for the center is to shape a narrative and core questions which Western societies need to address, especially with all the conflict within our societies over fake news and the like.

Mustonen: Shaping a credible narrative and framing the right questions is a core challenge but one which the Centre will hope to achieve in the period ahead.

"We are putting these issues in front of our participants and aim at improving our understanding of hybrid threats and the ways we can comprehensively response to the threats."

The Authoritarian Regime Approach

These two approaches – military enabled (hybrid war and "gray zone" con-ops) – and direct infrastructure engagement – lay a solid foundation for the authoritarian powers to engage effectively in information war, another key element of challenging the European democracies.

This challenge was the focus of a study published in 2018 written by Thomas Mahnken, Ross Babbage, and Toshi Yoshihara which was entitled "Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare." [1]

"Authoritarian regimes in Beijing and Moscow have clearly committed themselves to far-ranging efforts at political warfare that hope to achieve the ability to comprehensively coerce the United States and its allies.

"Only by clearly and frankly acknowledging the problem and organizing the respective governments to respond do we stand a chance of defending fee societies from these sophisticated efforts at manipulating public opinion and the decision-making pace of elected officials and government policy makers."

One of the authors of the report, Ross Babbage, discussed with us further how he looks at the challenge.

"For the liberal democracies, there is a pretty clear break between what we would consider war and peace.

"For the Chinese and the Russians, there is not quite the same distinction.

"They perceive a broad range of gray areas within which political warfare is the norm and it is a question of how effective it is; not how legitimate it is.

"They are employing various tools, such as political and economic coercion, cyber intrusion, espionage of various types, active intelligence operations and so forth."

Shaping a purely military response to the new challenges posed by direct defense in Europe is a necessary but not sufficient response to the threats posed by the 21st century authoritarian states.

Babbage went on to identify in the interview how we might repond.

What can we do to actually stop this and fix it?"

At present we are not telling the story of foreign political warfare broadly enough within our political and economic sectors.

We've got to improve our information operations. We need to throw sunlight on what these guys are doing and do so in a comprehensive and sustained manner.

Beyond that effort, I would identify a number of potential components of what one might call an effective counter strategy.

First is a denial strategy.

Here the objective is to deny, not just the operations and make them ineffective, but also to deny the political benefits that authoritarian states seek to win by conducting their operations.

Second is a cost imposition strategy.

We need to find ways to correlate their behavior with an imposed cost. We need to make clear that if they are going to behave like this, it will cost them in specific ways.

Third is focused on defeating their strategy, or making their strategy counterproductive.

We can turn their strategy on its head and make it counter-productive even within their own societies.

Their own societies are fair game given the behavior of the of our combined assets Russians and Chinese.

Fourth is to make it damaging, and even dangerous, for authoritarian regimes to sustain their political warfare strategy.

Authoritarian regimes have their own vulnerabilities and we need to focus on the seams in their systems to make their political warfare strategies very costly and risky.

And we need to do this comprehensively as democratic allies.

There's no reason why we can't coordinate and cooperate and make the most of our combined resources, as we did in the Cold War.

But do we have the right tools and coordination mechanisms for an all-of-alliance strategy to work well?

In my view, the Western allies have a great deal of work to do.

A Danish Perspective

During a conference held in Copenhagen on October 11, 2018, the Danish Minister of Defence provided an overview on how the government views defence and security, particularly challenges in direct defence of Denmark and Europe – cyberwar posed by Russia and the need to enhance infrastructure defence are of key concern.

The lines between domestic security and national defense are clearly blurred in an era where Russians have expanded their tools sets to target Western infrastructure. Such hidden attacks also blur the lines between peace and war.

Within an alliance context, the Danes and other Nordic nations, are having to focus on direct defense as their core national mission. This will mean a shift from a focus on out of area operations back to the core challenge of defending the homeland.

Russian actions, starting in Georgia in 2008 and then in the Crimea in 2014, have created a significant environment of uncertainty for European nations, one in which a refocus on direct defense is required.

Denmark is earmarking new funds for defense and buying new capabilities as well, such as the F-35. By reworking their national command systems, as well as working with Nordic allies and other NATO partners, they will find more effective solutions to augment defensive force capabilities in a crisis.

It was very clear from our visits to Finland, Norway and Denmark over the past few years, that the return to direct defense has changed as the tools have changed, notably with an ability to leverage cyber tools to attack Western digital society to achieve political objectives with means other than use of lethal force.

This is why the West needs to shape new approaches and evolve thinking about crisis management in the digital age. It means that NATO countries need to work as hard at infrastructure defense in the digital age as they have been working on terrorism since September 11th.

New paradigms, new tools, new training and new thinking is required to shape various ways ahead for a more robust infrastructure in a digital age.

Article III of the NATO treaty underscores the importance of each state focusing resources on the defense of its nation. In the world we are facing now, this will mean much more attention to security of supply chains, robust security of infrastructure, and taking a hard look at any vulnerabilities.

Robustness in infrastructure can provide a key defense element in dealing with 21st century adversaries, and setting standards may prove more important than the buildup of classic lethal capabilities.

A return to direct defense, with the challenge of shaping more robust national and coalition infrastructure, also means that the classic distinction between counter-value and counter-force targeting is changing. Eroding infrastructure with non-lethal means is as much counter-force as it is counter-value.

We need to find new vocabulary to describe the various routes to enhanced direct defense for core NATO nations.

A new strategic geography is emerging, in which North America, the Arctic and Northern Europe are contiguous operational territory that is being targeted by Russia, and NATO members need to focus on ways to enhance their capabilities to operate seamlessly in a timely manner across this entire chessboard.

In an effort to shape more interactive capability across a common but changing strategic geography, the Nordic nations have enhanced their cooperation with Poland and the Baltic states. They must be flexible enough to evolve as the reach and lethality of Russia's air and maritime strike capabilities increases.

Clearly, tasks have changed, expanded and mutated.

An example of a very different dynamic associated with direct defense this time around, is how to shape a flexible basing structure.

What does basing in this environment mean? Can allies leverage national basing with the very flexible force packages needed to resolve a crisis?

One of the sponsors of the Danish Conference was Risk Intelligence, provide a very cogent perspective on how to look at the challenge.

Their CEO, Hans Tino Hansen, a well-known Danish security and defense analyst explains the new context and challenges facing the Nordic countries:

"We need to look at the Arctic Northern European area, Baltic area, as one. We need to connect the dots from Greenland to Poland or Lithuania and everything in between. We need to look at the area as an integrated geography, which we didn't do during the Cold War.

"In the Cold War, we were also used to the Soviet Union and the Warsaw Pact being able to actually attack on all fronts at the same time, which the Russians wouldn't today because they are not the power that they used to be.

"And clearly we need to look beyond the defense of the Baltic region to get the bigger connectivity picture."

He went on to assert the need to rethink and rebuild infrastructure and forces to deal with the strategic geography that now defines the Russian challenge and the capabilities they have […] to threaten our interests and our forces."

Evaluating threats across a spectrum of conflict is the new reality. "We face a range of threats in the so-called gray area which define key aspects of the spectrum of conflict which need to be dealt with or deterred."

A system of crisis identification with robust procedures for crisis management will go a long way towards effective strengthening of infrastructure in the face of the wider spectrum of Russian tools.

"A crisis can be different levels. It can be local, it can be regional, it can be global and it might even be in the cyber domain and independent of geography. We need to make sure that the politicians are not only able to deal with the global ones but can also react to something lesser," Hansen says.

"The question becomes how to define a crisis.

"Is it when x-amount of infrastructure or public utilities have been disrupted or compromised?

"And for how long does the situation have to extend before it qualifies as a crisis?

"This certainly calls for systems and sensors/analysis to identify when an incident, or a series of incidents, amount to a crisis. Ultimately, that means politicians need to be trained in the procedures necessary in a crisis similar to what we did in the WINTEX exercises during the old days during the Cold War, where they learned to operate and identify and make decisions in such a challenging environment".

In short, the Russian challenge has returned – but in a 21st century context. that incorporates incredibly invasive infrastructure threats.

Direct defense strategies must include these threats as part of any comprehensive national security concept.

Strategic Communications and Resilience – Speech by Director Matti Saarelainen

"This morning I'm going to take my 10 minutes to talk about three things:1) How states and institutions can response to Hybrid threats effectively (and Strategic Communication's role in that)
2) Where EU and NATO can improve their response to Hybrid Threats
3) What the Hybrid CoE is doing to enable Member States and the institutions to build capability in this area

1. How: Given the theme of this conference I wanted to focus on the centrality of communication to effective Hybrid response. A few thoughts.

Separation anxiety- Strategic Communication suffers from a degree of separation anxiety- it is often treated as a separate field, with separate experts and communities. But at Hybrid CoE we see it as an intrinsic part of the response.

Effective resilience requires an open conversation with our population about unfolding Hybrid events (and our response to them) which maintains trust in our values, democratic processes and governance structures. Resilience also requires persuasive communications as we prepare our populations- campaigns which encourage them to change their behaviour and improve their own personal resilience are critical- whether we are asking them to put aside peanut butter or improve password security.

Separately, Effective deterrence of Hybrid threats requires States to demonstrate: resolve, coherence, capability, agility, willingness to attribute and desire to act in concert. To shape the adversary's perception, we need to make sure our actions are effectively communicated- to achieve ultimate impact. Our strategic communicators are best placed to do this.

All this speaks to the importance of strong- connective tissue between strategic communicators, policy makers and the intelligence community. They should not be an afterthought in the national or institutional crisis response structures. They should be at the policy making table, thinking not just about how to communicate the government or institution's response but what that response should be. They also need to be in close contact with the intelligence community. Strategic communicators often have a detailed understanding of the open source debate surrounding a Hybrid event (and access to the tools required to analyse it). Given the challenge of information sharing within and between governments open source material can and should be the bedrock of our resilience and deterrence strategy. A strong relationship between these two communities will ensure it is effectively leveraged.

2. Where: Mr. Chairman, you asked me to focus on where I think the EU and NATO response was strong and where there was room for improvements. Hybrid CoE has a unique perspective,

being neither EU, nor NATO and given one of our core goals is acting as a neutral facilitator between the two. A couple of thoughts on each.

On strengths, I want to pause a moment on vulnerabilities and values. Often the values which are central to these institutions: respect for human rights, strong democratic institutions, the market economy, freedom of speech and media and rule of law are singled out as intrinsic vulnerabilities. And there is no doubt many of these have been exploited by our adversaries for their own ends. But they are also the values with which we won the Cold War. They are in fact our strength. They form the foundation of our resilience as institutions (and the resilience of the member states within them). It is both glib and true to say we need to be better about communicating them.

On a more practical level, EU and NATO have developed a strong set of commitments and actions on countering Hybrid Threats. There is a good level of awareness of Hybrid and political will, at the most senior levels, to address it. The key now is to implement these effectively and and communicate that implementation with impact. While initiatives are key, it is their implementation which will shift the dial.

And with that I turn to a discussion on where the collective response could be improved… At our inauguration Commissioner King encouraged the Centre to be challenging… So, in that spirit a few areas for the EU and NATO to consider.

Hybrid threats are full spectrum in nature. The use of multiple means in coordination and with malign intent to achieve a political ends requires a coordinated response. At Hybrid CoE, when we talk about deterrence our underlying principle is that we will most effectively deny the benefit or impose cost on our adversary if all aspects of government and society are coordinated in their response. The same is true at the institutional level. Between them, EU and NATO have the capabilities to detect and respond to a hybrid attack. They also have the tools to effectively impose cost and deny benefit to the adversary. There is still a need at a strategic level to have discussions between the two organisations about using these capabilities and tools in a coordinated and coherent way, as part of a campaign to protect the values that are central to the institutions. So strategic level discussions about a coordinated response is key.

This however requires a whole of institution response to Hybrid within each organisation. The bureaucratic vulnerability, as we call it at the Centre is the single biggest spoiler in any actor's response to Hybrid threats. Siloes, blocks and poor information flow hampers response. On the EU side this means coherence between the Commission, EEAS, Council and Parliament and on the NATO side this is fusion across the civilian military divide. Both organisations are restructuring their approach to Hybrid internally, so we are keen to see the results. The logical extension of this is the creation of informal communities across the organisations (more on that later).

Agility is also key in cross institutional response and where there is always room for improvement at the national and institutional level. Particularly when it comes to crisis responses and political decision making. The PACE exercises have been key in exercising the organisations alongside each other. There is no substitute for exercising to test agility. Coherent and parallel exercising will remain important and the Hybrid CoE was pleased to support a joint NAC/PSC scenario-based discussion last autumn which tested this agility and provided an opportunity for a strategic discussion about a coordinated response. They will also support the exercises proposed as part of the Finnish EU Presidency.

Member States provide a key role in encouraging and supporting effective institutional response to Hybrid Threats. They also critical to overcoming some of the key barriers to closer institutional cooperation on Hybrid Threats. I continue to encourage all Hybrid CoE Member States to support their institutions in overcoming these barriers and being more ambitious in their implementation of these actions.

3. What the Hybrid CoE does to support the institutions and Member States to improve response.

In the last nearly two years we have focused our work in four key areas which we believe to be key to improving the Euro-Atlantic region's response to Hybrid threats.

Networks: We have built practitioner networks across our 20 member states, EU and NATO and the private sector. These networks train, exercise and share best practice with one another, as well as coordinating action and testing policy response options. We have practitioner networks on: energy, drones, maritime security, technology and hybrid warfare, strategic

communication, open source data, countering hostile states and legislative resilience. A networked response requires a networked solution.

Training: One of the Centre's core goals is to improve the capability of its member states to counter Hybrid threats. Training is an important way in which we do this. We have two flagship training events. One on using open source material to counter Hybrid threats. As I noted earlier, open source material is a critical enabler in building situational awareness and responding to Hybrid Threats. We train analysts and policy makers from across our Member States EU and NATO to analyse open source data and use it as part of their policy response to countering disinformation. We have run this course twice already and will run it on a further three occasions this year. This builds and supports our digital community of analysts across our 20 member states EU and NATO. We also train journalists to counter disinformation (with thanks to NATO support).

The second flagship training is on countering electoral interference. Elections, as I need not tell this community, are particularly susceptible to Hybrid attack. The two day event aims to bring together strategic communicators, intelligence and other government practitioners involved in securing elections- it and exercises them together. Facebook and Microsoft are our private sector partners. This roadshow will take place in six capitals this year.

Exercising and scenario based discussions are mainstreamed in most of our activities because they are so critical to ensuring agility and testing the ability to coordinate. We have held two strategic multinational exercises on Hybrid Threats with participation of our member states, EU and NATO. We have also held numerous subject specific exercises on everything from de-synchronisation of energy supply networks, to countering electoral interference (and in support of the Romanian Presidency last week hosted an exercise on mass casualties – to support EU and NATO crisis response). In addition to running our own exercises we run them for institutions- the NAC/PSC scenario-based discussion is a case in point. We also support others with scenario development.

Trend Mapping and Intellectual Matchmaking: There are plenty of actors out there willing to admire the problem but at Hybrid CoE we are actively engaged in trying to counter it. Trend mapping has been key to this. We have a unique methodology for doing this which brings nominated academic experts from across our Member States (we call them our expert pools) together with practitioners working on that topic to map emerging trends in the Hybrid landscape. In Madrid last week we held a trend mapping exercise in this academic/practitioner format behind closed doors on Russia. We find this intellectual matchmaking the most effective way of ensuring cutting edge academic thinking makes it into the policy making bloodstream.

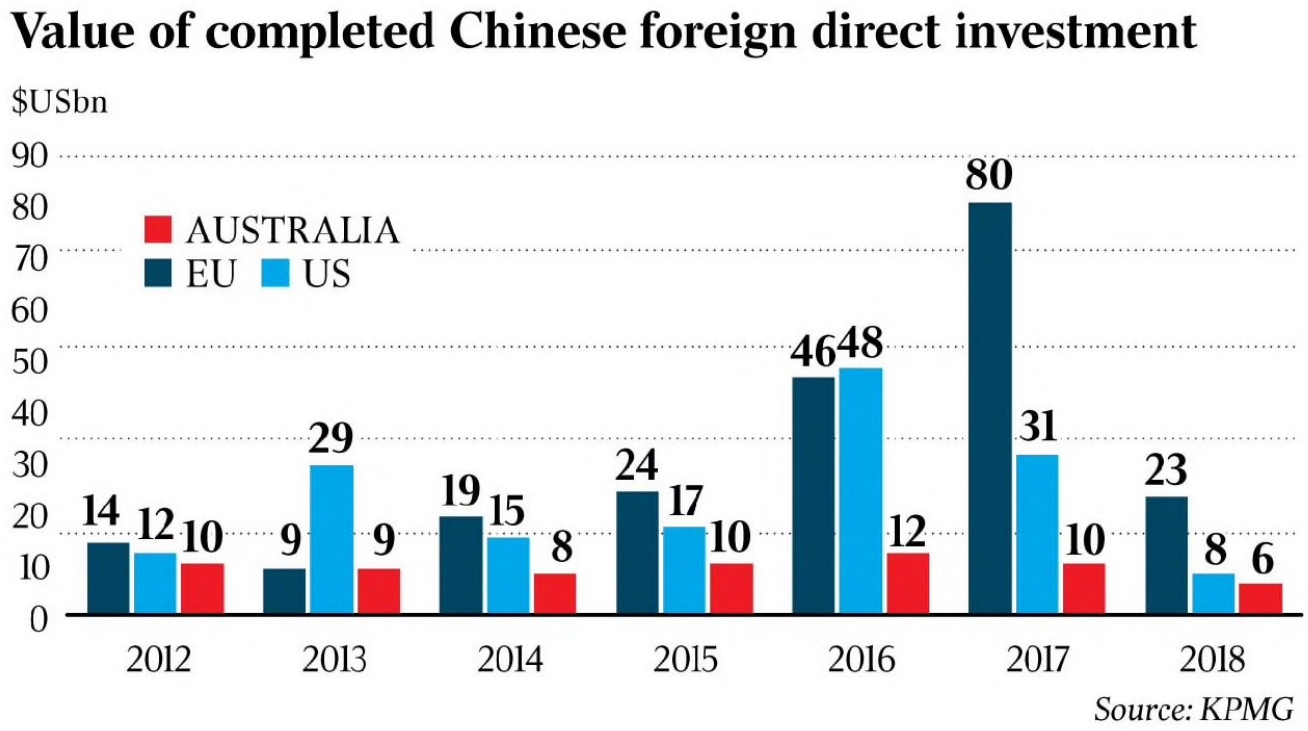
High Level Retreat: Finally, we host an annual EU/NATO high level retreat in Helsinki for senior leaders from both organisations. This outcome focused event gives staff from both organisations the chance to talk (beyond the confines of staff to staff cooperation) about emerging challenges and how the two institutions can develop a collective response.

It has been a pleasure to address you this morning. At the Centre we aim to lead the conversation on Countering Hybrid Threats. I look forward to hearing what follows."

China Shifts Direct Investment: Toughening Australian Regulations Have their Impact

04/07/2019

By defense.info



The impact of Chinese direct investment in Australia on Australian sovereignty has become an issue with increasing visibility.

The seminar this week in Canberra being held by The Williams Foundation is focus non the sovereignty issues for the ADF,

But there is the broader issues of the importance of having. an Australian National Security policy which can provide for greater capability to provide for enhanced sovereignty for Australian infrastructures as a key national effort.

According to an article by Glenda Korporaal published in The Australian entitled "Chine Invest Less as FIRB Toughens Up."

China's new investment in Australia has fallen sharply as a result of tighter foreign investment scrutiny in Australia and overseas investment policies in China favouring Belt and Road projects, according to a survey to be released today by KPMG and the University of Sydney.

The survey shows that new investment from China was down by more than 36 per cent last year to $8.3 billion, with a big fall in investments by Chinese state-owned enterprises (SOEs), which face tougher scrutiny from the Foreign Investment Review Board and regulators.

The article quotes Doug Ferguson, KPMG's head of Asia and International Markets, with regard to the sharp fall in investment in Australia despite an overall increase in Chinese overseas investment overall.

Ferguson is quoted as follows:

"Money in China has been allocated to Belt and Road countries through central Asia and east Asia, while some countries like France, Spain and Sweden have also had an increase.

"It has been largely the countries that have been recipients of BRI investments which have done well out of new Chinese investments in 2018," he said.

Huawei, 5G Networks: ASPI Provides a Case Study With Regard to Restoring Infrastructure Sovereignty

04/06/2019

With 2014 came the end of an era.

It was apparent that authoritarian powers were back and in many ways' ascendant.

The response by the liberal democracies has been varied and differentiated.

Some have taken it seriously; others hope that the past period of hope for a globalized democratization process will return.

Nonetheless, the challenge of the 21st century authoritarian powers needs to be addressed as a core one, not simply as an aberration of globalization and the return at some time in the near future the inevitable march to global democratic capitalism.

There are two prongs of the challenge to focus on reality.

The first is building a crisis management force structure which allows for engagement at the low end and escalation dominance throughout.

We have argued that the kill chain concepts of operations which are a work in progress provide a core way ahead to shape such a force.

This is necessary but not sufficient approach to defend our societies against the 21st century authoritarian powers.

The second prong is even more challenging – it is to build secure infrastructure in the liberal democracies.

Given the nature of the global system in commodities like IT and communications, national efforts can provide security for sovereign solutions, but only up to a point.

We no longer have national drafts in most Western states.

But mobilizing support for robust and secure infrastructure is the functional equivalent to a national draft to mobilize the nation against the innovative approaches being taken by 21st century authoritarian powers, approaches designed to undercut our way of life and to protect themselves from any counter measures we might take.

This is not about the global market or globalization glorified by the global consulting firms; this is about a strategy to deal with 21st century authoritarian powers exploiting the global markets abroad, while protecting themselves at home, as part of a dominance strategy.

Getting governments to work with industry and society to limit the penetration of authoritarian states within the internal processes of our societies is crucial to shape a more secure and safe liberal democratic systems.

The problem is that the ability of the authoritarian states to operate within our societies has been and is being facilitated by their ability to own or participate in the development of our core infrastructures.

Shaping a more robust and resilient infrastructure for the liberal democracies starts as a national endeavor, but requires cross national cooperation among the liberal democracies to achieve long term success.

Sovereignty in this case can be only semi-sovereignty but if a nations' control disappears through "market forces" being exploited by the authoritarian states then sovereignty simply disappears and with it the ability to defend our societies militarily when the time comes in a crisis.

A case in point is how the Chinese Government is using the global reach of Huawei to own and shape infrastructure in the liberal democratic states to their advantage.

A 2018 report by the Australian Strategic Policy Institute has provided an excellent over to the overall challenge being posed by Huawei and explanations of why the Australian government has acted to restore Australian control for their communications networks.

This obviously is not a one off, and must become part of a broader Australian redesign of infrastructure policy to be built on foundations which ensure a more robust and resilient Australia, but it is a clear beginning.

As Elsa Kania notes in the report:

In Xi Jinping's China—it's worth raising the question of whether any Chinese company has adequate freedom to 'go its own way,' particularly on issues that are sensitive or strategic. In the absence of true rule of law, even those companies that may wish to resist impositions by the state on their commercial interests have fewer avenues through which to do so.

Meanwhile, there's also a new legal basis that the Chinese government could use to mandate Huawei's compliance with state security interests that may be contrary to corporate imperatives. Notably, in China's National Intelligence Law (国家情报法), released in June 2017, Article 7 declares:

All organizations and citizens shall, in accordance with the law, support, cooperate with, and collaborate in national intelligence work, and guard the secrecy of national intelligence work they are aware of. The state will protect individuals and organizations that support, cooperate with, and collaborate in national intelligence work.

Similarly, Article 12 highlights that national intelligence agencies may 'establish cooperative relationships with relevant individuals and organizations, and entrust them to undertake relevant work'.At the same time, the law itself is ambiguous as to the scope and bounds of what 'intelligence work' may entail. Pursuant to this framework, there appears to be a direct obligation on the part of Huawei—or any other Chinese company or citizen for that matter—to assist the activities of Chinese state intelligence services.

Ultimately, the 'much ado' about Huawei is arguably justified, not so much because Huawei is Huawei but rather because of nature of the CCP and the framework for Chinese intelligence operations. In this regard, the anxieties and uncertainties about Huawei are similarly applicable to any Chinese company operating with this system, absent rule of law and without full transparency.

Danielle Cave then added:

It's a double-edged sword for China. Requiring individuals and organisations to support, cooperate with and collaborate in intelligence activities, of course, comes at a cost. And that cost will be the international expansion plans of Chinese companies—state-owned and private— which have been well and truly boxed into a corner with this law.

The CCP has made it virtually impossible for Chinese companies to expand without attracting understandable and legitimate suspicion. The suspicion will be deeper in countries that invest in countering foreign interference and intelligence activities. Most developed countries, including Australia, fall into that category.

This fascinating tension—between commerce and intelligence collection—will only intensify and will eventually force some tough decisions. What's more important to the CCP? Using Chinese companies operating overseas to collect intelligence or supporting the international success of those companies?

A little from column A and a lot from column B is probably the ideal mix for any government.

But betting big and hoping for roaring global success on both fronts is a crucial mistake. The two just don't go hand in hand. There will be a loser. And this year, at least in Australia, it will be Huawei.

Peter Jennings, the director of ASPI, looked at more than Huawei but at other Chinese efforts in Australia and argued:

The national security calculation for Australia is hardly less stark for the gas and electricity sector as it is for telecommunications.

Can we afford to let the bulk of that critical infrastructure be owned and run by a company that is ultimately subject to an authoritarian one party state with a massive intelligence apparatus and an equally large cyber force within the PLA looking for national vulnerabilities that might offer exploitable advantage?

Since the Ausgrid decision not to sell NSW's 'poles and wires' to State Grid or CKI, a Critical Infrastructure Centre was created by the Federal Government and a new Security of Critical Infrastructure Act passed by Parliament in 2018 showing that more attention is being paid to how Australia can protect critical infrastructure, particularly from malicious cyber interference.

It's true that one does not need to own an asset to be able to damage it through cyber manipulation, but hands-on access to the hardware and software of the industrial systems running our critical infrastructure is a clear vulnerability. The non-negotiable interaction of Chinese intelligence services with their business community remains a persistent challenge.

The non-national security problem for CKI remains what Treasured Scott Morrison has called the 'aggregation effect' of an ever larger part of Australia's energy infrastructure being owned by a small number of mainly Chinese and Hong Kong businesses.

The Government has warned on a number of occasions that 'Australia's national critical infrastructure is more exposed than ever to sabotage, espionage and coercion.'

The statement is not lightly made and we should take it seriously.

As difficult as these decisions are, Canberra should move quickly to block Huawei's access to 5G and CKI's access to APA's gas and electricity business.

This is the necessary price of maintaining national security interests in the face of an increasingly predatory China looking to maximise its own strategic interests at the expense of all others.

The Australian government in 2018 did ban two big Chinese telcos—Huawei and ZTE—from selling 5G in Australia.

Michael Shoebridge argued that this effort needs to be part of a wider effort.

Australia's decision has been received in odd and expected ways in Beijing. The first, odd, reaction was in the Communist Party's strident mouthpiece, the Global Times, expressing disappointment that Australians won't get cheap Huawei services.

That swiftly moved to more predictable if concerning statements, also in the Global Times, such as 'Canberra stabs Huawei in the back' and 'those who willfully hurt Chinese companies with an excuse of national security will meet their nemesis'.

The Global Times claimed Huawei is 'a company that embodies China's reform and opening up'. China's leaders know this is disingenuous. Beijing's track record on 'opening up' to non-Chinese providers is of partnerships subject to deep control by Chinese authorities and technology transfer to the Chinese entities.

More interestingly, the article asked, 'Will the move cause a domino effect in Western countries?' This gets to a real concern for China's leaders about the precedent effect of the US and Australian decisions.

These fit with rising global concern about how the Chinese state is using its power. Chinese assertiveness under President Xi Jinping's One Belt, One Road China-centred infrastructure initiative has provoked unease in countries from Sri Lanka to Malaysia, and even Tonga.

Add to this the glimpses we are gaining into China's use of digital technologies through 'social credit' to control its citizens and its electronically enabled surveillance and repression of millions of Uyghurs.

So, Xi is right to worry if the reality of the Communist Party in action looks very different from the 'win–win' words of his 'China Dream'. This goes well beyond the Australia–China relationship.

Morrison has set a course in managing the relationship that will welcome our valuable two-way trade in resources and services, based on us selling world-class items that China needs at globally competitive prices.

But he's also laid out clear markers that where our national interests differ—as they do in questions of deep access to, and potential control of, our critical infrastructure—he will put national interests first.

Refreshingly, he won't pretend that repetition of slogans such as 'win–win' and 'mutual benefit' will make everything okay, even if it's the 'correct line' that Beijing wants to hear.

The future directions for broader economic and technology policy seem clear. They align with the government's big strategic direction to work with partners to advance a 'free and open Indo-Pacific'.

This is a vision of broad economic and security partnerships, not deep dependency on single markets and partners. That drive towards economic diversification is one we'll probably hear a lot more of as the new Morrison government gets underway.

The report can be found at the following link on ASPI's website:

https://www.aspi.org.au/report/huawei-and-australias-5g-network

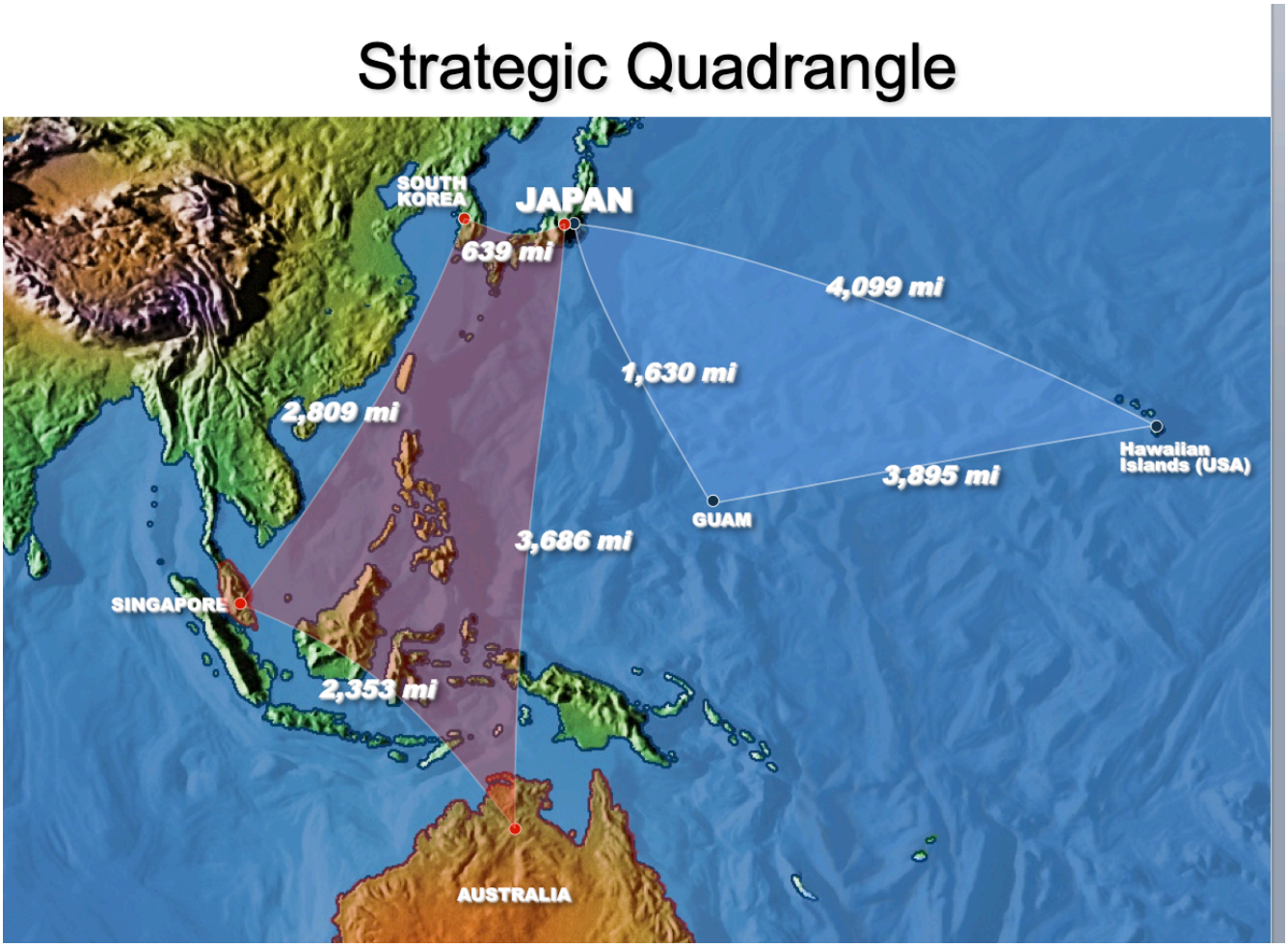
We will be publishing more recent pieces by ASPII on this crucial issue on defense.info from time to time.

We applaud ASPI for taking on this crucial issue and look forward to expanding the infrastructure more broadly in both Pacific, American and European calculations in shaping an effective strategy to dissuade, deflect, deter and to defeat the efforts of the new authoritarians.

The defeat side will not happen unless we take the information war back within the walls of their own societies.

Full-Spectrum Crisis Management for the Liberal Democracies: Crafting a Kill Web Force

04/02/2019



As the strategic shift from the land wars gains momentum the investments and training in an appropriate 21st century crisis management and high intensity combat force will not be modelled on the Cold War European based force. It is not about a German-US Army brotherhood with significant presence. It is not about re-establishing air-land battle

It is about leveraging core force integration capabilities, such as F-35 with the Aegis, which can provide a pull function moving the US and the allies towards a more flexible and scalable force which can operate over the spectrum of operations.

As Vice Admiral Barrett, the former Chief of the Australian Navy highlighted with regard to how he saw the build out of the Australian Navy: "We are not building an interoperable Navy; we are contributing to an integrated Australian Defence Force able to exercise sovereign options and work closely with core allies."

Because the adversaries are building to mass and are emphasizing expansion of strike capabilities controlled by a very hierarchical command structure, the kind of force which will best fit Western interests and capabilities is clearly a. distributed one. Fortunately, the technology is already here to build effectively down this path, a path which allows engagement at the low end and provides building blocks to higher end capabilities.

The force we need to build will have five key interactives capabilities:

1. Enough platforms with allied and US forces in mind to provide significant presence;
2. A capability to maximize economy of force with that presence;
3. Scalability whereby the presence force can reach back if necessary at the speed of light and receive combat reinforcements;
4. Be able to tap into variable lethality capabilities appropriate to the mission or the threat in order to exercise dominance.
5. And to have the situational awareness relevant to proactive crisis management at the point of interest and an ability to link the fluidity of local knowledge to appropriate tactical and strategic decisions.

To be blunt about the last point – a cutting edge new system, the Triton UAV, is part of the new maritime SA force for the US and slelected allies. The SA on this aircraft needs to be used by the presence forces and not be part of the "intelligence collection" team back in the United States. Or put in other words, the new challenges require a significant challenge in terms of how the very un-agile US intelligence process tries to "own" information.

The new approach is one which can be expressed in terms of a kill web, that is a US and allied force so scalable that if an ally goes on a presence mission and is threatened by a ramp up of force from a Russia or China, that that presence force can reach back to relevant allies as well as their own force structure.

The inherent advantage for the US and its allies is the capability to shape a more integrated force which can leverage one another in a crisis.

A good example has been the evolution of the Aegis fleet in the Pacific.

The enhanced capability of the US and allied navies is coming not just from platforms but from kill web integration.

There is no greater case in point than how the US Navy and the allies are integrating their Aegis destroyers.

Earlier, this year, the Australian Navy demonstrated its ability to integrate with the US Navy with regard to the CEC system.

According to Andrew McLaughlin in an article published on January 7, 2019:

The tests were conducted in conjunction with the US Navy at the vast Pacific test ranges near Hawaii and off the coast of California, and saw the vessel's systems and crew challenged in realistic tests and demonstrations. This included testing the vessel's ability to integrate with US Navy assets via the Co-Operative Engagement Capability (CEC), a US high-end naval networking capability so far made only available to Australia.

"We were presented with some of the world's toughest and most challenging threats; modern anti-ship missiles, maritime strike aircraft, fighters and high-speed attack craft," Commanding Officer of HMAS Hobart, CAPT John Stavridis told Navy Today. "On every occasion we successfully defended all threats."

Part of HMAS Hobart's systems validation included a series of at sea tests known as Combat System Ship Qualification Trials (CSSQT) which aim to achieve a sustainable level of combat and weapon system readiness.

"This ship represents the future of the Royal Australian Navy's surface combatants: capable, competent and lethal," Fleet Commander, RADM Jonathan Mead said upon HMAS Hobart's return to Sydney. "With her recently commissioned sister ship, HMAS Brisbane, and soon to be delivered NUSHIP Sydney they will be able to defend our Fleet against any threat."

As part of the increasingly integrated maritime threesome — the US, Australian and Japanese Navies — the Japanese recently added a new platform to the mix.

According to Naval Today:

Japan's second Asahi-class destroyer, the JS Shiranui, entered Japan Maritime Self Defense Force (JMSDF) service in a ceremony at Mitsubishi Heavy Industries' Nagasaki Shipyard on February 27.

The lead ship in the class was commissioned a year before, on March 8, 2018.

The 5,100-ton general-purpose escort destroyers were previously designated as 25DD and are designed on the basis of Akizuki-class destroyers but with a focus on anti-submarine instead of anti-air warfare.

JS Shiranui (DD-120) was launched in October 2017 and was commissioned without delays.

Asahi-class destroyers are lauded as fuel-efficient ships featuring COGLAG, a combined gas turbine engine and electric propulsion system. They measure 151 meters in length and reach speeds of 30 knots, according to the Japan defense ministry. Armament includes Mark 41 vertical launch systems for self protection, 62-caliber naval guns, close-in weapon systems and two Mark 32 surface vessel torpedo tubes.

The destroyers will have a complement of around 230 and embark one Mitsubishi-built SH-60J/K are anti-submarine patrol helicopter.

Asahi-class destroyers are the first JMSDF ships to deploy with periscope detection radars in addition to being equipped with new towed array sonars.

Earlier, when the first of the new destroyers was launched from its shipyard last year, the integration piece was highlighted.

Japan launches first 27DDG-class AEGIS destroyer from a shipyard in Yokohama today (July 31). She has named "Maya" after mountain in Japan and WWII heavy cruiser.

The US$1.5 billion vessel is the seventh Aegis destroyer acquired by Japan Maritime Self-Defense Force, but the first to be fitted with the advanced Cooperative Engagement Capability (CEC) system. With a displacement of 8,200 tons and a length of 170 meters, it is scheduled to enter service by 2020.

Supplied by the US, the CEC system enables real-time sharing of intelligence on battlefield situations and hostile targets between ships in allied navies, while information and parameters are synced across all platforms linked to a sensory network. Sharing of radar and fire-controlling data will also be possible with the US Navy.

Warships equipped with this system can intercept incoming ballistic missiles in steep, lofted trajectories, and track dozens of targets simultaneously while firing clusters of defensive missiles, according to Japan Times. One such missile is the SM-3 Block IIA.

Japan will have eight Aegis destroyers with a ballistic missile defense capability by 2021. At their core will be a computer-based command-and-decision element capable of mounting simultaneous operations against a range of threats.

Because all three of these navies are part of the F-35 global enterprise as well, integration of F-35s with Aegis is part of the combat capability facing adversaries in the Pacific.

A shift to a kill web approach to force building, training and operations is a foundation from which the US and its allies can best leverage the force we have and the upgrade paths to follow. A kill web linked force allows a modest force package – economy of force – to reach back to other combat assets to provide for enhanced options in a crisis or to ramp up the level of conflict if that is being dictated by the situation.

The evolution of 21st century weapon technology is breaking down the barriers between offensive and defensive systems. Is missile defense about providing defense or is it about enabling global reach, for offense or defense? Likewise, the new 5th generation aircraft have been largely not understood because they are inherently multi-domain systems, which can be used for forward defense or forward offensive operations.

Indeed, an inherent characteristic of many new systems is that they are really about presence and putting a grid over an operational area, and therefore they can be used to support strike or defense within an integrated approach.

In the 20th Century, surge was built upon the notion of signaling. One would put in a particular combat capability – a Carrier Battle Group, Amphibious Ready Group, or Air Expeditionary Wing – to put down your marker and to warn a potential adversary that you were there and ready to be taken seriously. If one needed to, additional forces would be sent in to escalate and build up force.

With the new multi-domain systems – 5th generation aircraft and Aegis for example – the key is presence and integration able to support strike or defense in a single operational presence capability. Now the adversary cannot be certain that you are simply putting down a marker.

This is what former Air Force Secretary Michael Wynne calls the attack and defense enterprise.

The strategic thrust of integrating modern systems is to create a grid that can operate in an area as a seamless whole, able to strike or defend simultaneously. This is why Wynne has underscored since at least 2005 that fifth generation aircraft are not merely replacements for existing tactical systems but a whole new approach to integrating defense and offense.

When one can add the strike and defensive systems of other players, notably missiles and sensors aboard surface ships like Aegis, then one can create the reality of what Ed Timperlake, a former fighter pilot, has described as the F-35 being able to consider Aegis as his wingman.

By shaping a tron warfare system inextricably intertwined with platforms and assets, which can honeycomb an area of operation, an attack and defense enterprise can operate to deter aggressors and adversaries or to conduct successful military operations.

The US Navy leadership has coined their version of this approach, the "kill web." In an interview we did with Rear Admiral Admiral Manazir, then head of N-98, Naval Aviation.

If you architect the joint force together, you achieve a great effect.

It is clear that C2 (command and control) is changing and along with it the CAOC (Combined Air and Space Operations Center).

The hierarchical CAOC is an artifact of nearly 16 years of ground war where we had complete air superiority; however, as we build the kill web, we need to be able to make decisions much more rapidly.

As such, C2 is ubiquitous across the kill web.

Where is information being processed?

Where is knowledge being gained?

Where is the human in the loop?

Where can core C2 decisions best be made and what will they look like in the fluid battlespace?

The key task is to create decision superiority.

But what is the best way to achieve that in the fluid battlespace we will continue to operate in?

What equipment and what systems allow me to ensure decision superiority?

We are creating a force for distributed fleet operations.

When we say distributed, we mean a fleet that is widely separated geographically capable of extended reach.

Importantly, if we have a network that shares vast amounts of information and creates decision superiority in various places, but then gets severed, we still need to be able to fight independently without those networks.

This requires significant and persistent training with new technologies but also informs us about the types of technologies we need to develop and acquire in the future.

Additionally, we need to have mission orders in place so that our fleet can operate effectively even when networks are disrupted during combat; able to operate in a modular-force approach with decisions being made at the right level of operations for combat success.

Inherent in such an enterprise is scalability and reach-back.

By deploying the tron warfare grid or a C2/Information superiority "honeycomb", the shooters in the enterprise can reach back to each other to enable the entire grid of operation, for either defense or offense.

By being able to plug into the F-35 and Aegis enabled honeycomb, the United States providees force augmentation and surge capability to those allies and at the same time those allies enable forward deployments which the United States would not own or operate.

Put in other terms, presence is augmented at the same time as scalability is as well. This provides a significant force multiplier across the crisis management spectrum.

In effect, what could be established from the United States perspective is a plug-in approach rather than a push approach to projecting power. The allies are always forward deployed; the United States does not to attempt to replicate what those allies need to do in their own defense.

But what the United States can offer is strategic depth to those allies. At the same time if interoperability and interactive sustainability are recognized as a strategic objective of the first order, then the United States can shape a more realistic approach than one which now rests on trying to proliferate power projection platforms, when neither the money nor the numbers are there.

Put bluntly, if you do not get, you do not get it. The fifth generation enabled force is here; and the challenge is clearly to leverage it as one builds out new elements of the kill web to enhance the scope and lethality of the US and allied force structure in either the Pacific or Europe.

For our recently published Special Report which looks at these issues, please see the following:

the-strategic-shift-the-role-and-impact-of-the-f-35-global-enterprise