Irregular Warfare in Strategic Competition and Gray Zones: Prosecuting Authoritarian Subversion and Exploitative Use of Corruption and Criminality to Weaken Democracy

David M. Luna
Executive Director
International Coalition Against Illicit Economies (ICAIE)
Strategic Multi-Layer Assessment (SMA) Speaker Session
U.S. Department of Defense
The Pentagon
Washington, DC
22 August 2024

Good morning.

Colleagues, it is a great honor to be here with you to participate in this SMA Speaker Series to talk about the increasingly more complex geo-political challenge of irregular warfare (IW) in gray zones. These challenges are related to how our military adversaries such as China, Iran, and Russia are manipulating chaos, instability, and insecurity including, for example through co-option and coercive economics, and by:

- weaponizing corruption including election interference through illicit financial flows to support pro-authoritarian candidates that advance malign influence operations by exploiting governance gaps to secure friendly policies and win new anti-West friends, while harming U.S. national interests;

- leveraging criminal networks, state-sponsored armed and violent proxies, diasporic communities, and professional super-fixers (enablers) to achieve military objectives, including to spread democratic backsliding, and to destabilize the national security interests of the United States and those of our democratic allies; and

- advancing revisionist and revanchist policies to construct their vision for a multi-polar world, exploiting gray zones from small islands in the Asia Pacific region to fragile democracies in Latin America, Africa, and Southeast Europe.

As I will outline in this presentation, we remain unprepared for irregular warfare. China, Iran, and Russia continue to seek to undercut U.S. influence, degrade American relationships with key allies and partners, and exploit the global environment to their advantage including by leveraging, and exploiting – as instruments of competition – strategic corruption, illicit vectors, criminal activities, economic coercion, malign influence operations, terrorism, guerilla warfare, insurgency, sabotage and subversion through asymmetrical and clandestine efforts.

It is vital that we astutely manage escalation dynamics in global competition scenarios to dictate the costs related to hostile actions by effectively prosecuting the strategic use of corruption and predatory criminality by our adversaries across gray zones to win the peace and to ensure that democracy reigns over authoritarianism.

Critically, the rule of law and the international rules-based system must outlive targeted chaos, subversion, and malign influence operations in some of today's contested security landscapes and ongoing great power competition (GPC).

I also think that we must view such current and horizonal threats through a prism of threat convergence so that we may develop actionable responses to counter illegality corroding the rule of law, and inter-connected illicit threat networks more robustly, and integrate such law enforcement disciplines into DOD's irregular warfare planning and strategies.

Through this framework, I firmly believe that we can better help DoD, IC, and inter-agency communities; our Combatant Commanders, and warfighters to understand the threat intelligence overlays of global ecosystems of criminality and corruption, and to equip them with a sharper set of:

- Pragmatic resource-sustainable IW tools and anti-crime capabilities,
- greater data analytics and data mapping; and
- leveraged innovation and technological capacities including AI and quantum computing.

These tools will help them to not only develop more dynamic national security military strategies, but to get ahead of the game in planning for future irregular warfare campaigns, using smarter IW capabilities to expand the competitive space to our advantage, and counter illicit operations against poly-threat networks to defeat American adversaries' own competitive strategies.

To meet the GPC challenge, it is vital that we seize the initiative while being cleared-eye and see the shadowverse – where everything is connected – as a hybrid battlefield that is being primed and executed by our enemies to destabilize American and Allied power from within, our markets and prosperity, the rule of law, and democracy itself.

After sharing a snapshot and insights of some of the emerging hot spots and gray zones of concern around the globe, I hope to illuminate my principal policy thrust of threat convergence in a criminalized multi-polar world being created by China, Iran, North Korea, Russia, and other malevolent state and non-state actors: I will pivot to discuss possible tools, capabilities, and capacities that can be brought to the fight, including to foster unified action with allies and partners including a proposal for establishing Special Action Task Forces to counter malign influence and strategic corruption and criminality; and more importantly, ways to develop IW strategies to secure the peace in the current geopolitical environment.

Crime and Corruption as IW Instruments to Weaken Democracies in Gray Zones

A few months back I had the distinct pleasure of delivering a keynote address to a meeting hosted by DoD's Offices for Special Operations/ Low-Intensity, Counter Low-Intensity (SO/LIC), and DoD Counternarcotics and Counter Transnational Organized Crime (CTOC) Program which focused more on the specific illicit threat networks.

- With today's presentation, I will sharpen that earlier threat assessment and focus more on policy actions that need to be integrated into irregular warfare strategies.

During my close to 20 years at the State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL),

- I worked across the inter-agency and national security community to craft national security strategies and initiatives in the fight against corruption, organized crime, and illicit threats.

- These efforts worked to optimally leverage collective energies across borders with unique authorities, programs, and resources to do more together; and

- in support of our law enforcement and defense communities to combat transnational crime and security threats.

Last month, the Office of the Director for National Intelligence (ODNI) released a brief report, "Conflict in the Gray Zone: A Prevailing Geopolitical Dynamic Through 2030", highlighting how:

- through 2030, great power competition and international relations generally will increasingly feature an array of hostile "gray zone" activities as China, Iran, North Korea, and Russia seek to challenge the United States and gain advantage over other countries through deliberate campaigns, while also trying to avoid direct war.

- These gray zones are more often than not exploited in places where corruption thrives, and criminals finance chaos, impunity, and insecurity.

Today I will focus on numerous "gray zone" geopolitical attacks in the current fragile global order, in which China, Iran, Russia, and others, are leveraging, and financing:

- greater strategic corruption and ecosystems of criminality to advance a multi-polar agenda that challenges longstanding rules of the international system with alternative forms of governance;

- and using illicit measures and criminally-oriented proxies to simultaneously promote authoritarianism and weaken democracies, erode institutions, and undermine law and order.

While they may have distinct approaches, they share similar goals by amplifying or reinforcing each other's active measures intended to prime and soften up political systems, and lead to the collapse and co-option of governments. 1

- China, Russia, and Iran are working to gain control over strategic locations, critical minerals, ports, and infrastructure with an aim of becoming forward operating bases for their military's expeditionary forces and intelligence agencies (e.g., Islands in the Pacific) and corrode American influence in the country, sub-region, and diplomatic circles.

These days, ICAIE is working with partners to undertake cutting-edge research to map threat networks to help the US and allied governments, the private sector, and committed trusted partners to:

- see the inter-connections of illicit vectors;
- pinpoint the nodes of crime convergence;
- identify gray zones exploited by malign state actors and proxies to discredit democratic institutions;
- track illicit trafficking routes, supply chains, and illicit financial flows; and
- strategically piece together the cascading effects of today's spectrum of threats in an ecosystem of criminality and corruption.

We hope that these threat intelligence overlays will drive further analysis and investigations to disrupt illicit threat networks and their enablers corrupting governments and weaking democracies.

- Because the reality is that our adversaries are in fact leveraging strategic corruption and criminality in gray zones to thwart U.S. foreign policy goals, without embarking on large scale kinetic military conflicts or worrying about cross-border law enforcement prosecutions.

Global Illicit Environment in a World of Convergence

At the onset, let me emphasize that despite many successes of law enforcement, the global ecosystem of criminality and corruption has expanded greatly today compared to even a decade ago, fueled by criminal opportunists and profit driven-illicit entrepreneurial networks and kleptocrats. These malign actors are:

working feverishly to exploit a multitude of lucrative illicit economies, which constitutes about 7-15% of the world's economy – or over $20 trillion a year – going toward criminal networks.

- Equally concerning: global criminality and corruption have also expanded with global trade;

  and now enable great power competitors and adversaries, such as Russia, China, and Iran, North Korea to underwrite armed conflicts and malign operations against Western democracies and free markets.

Moreover, among the reason local conflicts no longer end is that they are supported by illicit networks.

- Paramilitary groups supported by criminal opportunists and profit-driven illicit companies exploit conflict and instability to expand criminal economies.

- In fact, rampant corruption and the violence wrought by organized criminal and terrorist networks help to soften the conditions for insecurity that are exploited by authoritarian states to weaken other fragile governments.

State capture aided by criminality and strategic use of corruption results in democracies sliding into autocracies, and through proxies, helps to start or expand armed conflicts and regional insecurity, and even, to establish disinformation platforms that sow divide within democratic states.

Russia

- For example, Russia's Wagner Group had assisted in a series of coups in Africa, that have brought some juntas to power or enabled further kleptocracies to reign;

  - In exchange, Russian proxies now run gold and diamond mines, high value timber and other natural resources and commodities (e.g., cocoa, coffee, sugar) in those countries, and allow for autocrats to remain in power.

- From the Central African Republic (CAR) to Mali, Niger and Sudan, Wagner's successors – African Corps – continue to employ active measures to disrupt Africans' efforts to move their countries from violent conflict to stability, by moving money and weapons around the continent through an intricate web of shell companies, and through criminal networks specializing in illicit trafficking, illegal trading, and sanctions busting.

- What results is chaos, furthering the corruptive influence of extremist insurgencies in many cases, and regime protection of authoritarian (mostly military-led) rulers that face sanctions and condemnations on their human rights abuses.

- Some of the dirty profits derived by Russian mercenaries in Africa have helped Russia bypass global sanctions to fund its war in Ukraine and supported political upheavals and paramilitary mis-adventures in the Middle East, Balkans, and former Soviet republics.

- In Latin America, Russian proxies are selling some of the more advanced surveillance technologies to state and non-state criminal actors across the hemisphere, greatly enhancing their ability to monitor and attack political enemies, law enforcement, journalists, human rights workers and anyone else they perceive as a threat.

- And as many experts have correctly pointed out, Russia remains a criminalized state led by a ruthless and thuggish "Godfather".

- The Russian mafia is an extension of the Putin regime in advancing Russia's national interests overseas and an instrument of its power, operating in the shadows as illicit facilitators and super fixers to other criminal networks and authoritarian governments around the world.

- Russian cyber criminals not only penetrate businesses to steal trade secrets and funds, but to also launch cyberattacks against enemies of the Kremlin, and further extort, exert control, and expropriate wealth through extortion, corporate raid forces, or financial fraud schemes.

- The Silo-viki too may be asked to engage in kidnappings and assassinations on behalf of their masters in Moscow.

- Finally, one last point on Russia: While annexation of Crimea and the recent invasion of Ukraine has significantly affected regional illicit economies,

  Russian criminal networks continue to aid Russian intelligence and special forces in smuggling needed weapons and technologies (e.g., missiles, artillery shells, and microchips).

  This undermines Western sanctions and export bans for highly-sought consumer goods, and helps to launder assets for oligarchs in places like Dubai, London, New York, and other Western capitals.

China

Now let me focus for a few minutes on a bigger threat, China. FBI Director Christopher Wray has underscored in recent years that China remains the "biggest threat" to our national security and homeland.

- This is not only because of its global power ambitions, and active involvement in transnational crimes, but also its political interference operations, as Secretary of State Antony Blinken underscored a few months ago.

    - China's involvement in expanding illicit economies around the globe has had a triple whammy effect. It:

        1) increases tremendous illicit wealth for its ruling CCP elite;

        2) hurts U.S. national security, American competitiveness, and innovation; and

        3) finances China's global ambitions to become the predominant superpower by 2049 in a multi-polar world, a goal that President Xi Jinping has openly stated.

In fact, ICAIE has in recent years reported on how CCP Inc. has leveraged corruption, illicit markets, and predatory trade and lending practices to become the world's largest player in almost every major sector of transnational crime including:

- counterfeits, trafficking in weapons, humans, wildlife, illegally-harvested timber, fish, and natural resources, theft of IP and trade secrets, illicit tobacco, organ harvesting, and other crimes.

Several trillion U.S. dollars in illicit proceeds every year are generated from predicate offenses for money laundering that touch China's jurisdiction and markets, and are often used to finance China's authoritarian regime.

According to this ICAIE report, China may very well be the biggest money laundering hub in the world and the CCP Inc. one of most profitable transnational illicit trade syndicates.

- On so many fronts, China poses a serious geopolitical and CTOC threat, given its proclivity to make money on crime and the laundering of dirty monies of drug cartels, kleptocrats, terrorists, sanctioned rogue states and pariahs, and

- Also, through asymmetrical maneuvers, to steal Americans' personal identifiable information (PII), trade secrets, and intellectual property, as well as finance its foreign malign influence campaigns against the United States.

- China also has helped Russia, Iran, and others evade international sanctions, including on oil exports.

These Chinese threats will require even more attention as numerous illicit industries driven by China (and Chinese triads) continue to expand including across Latin America.

- In Panama, for example, China is leveraging bribery of government officials to win concession rights to control the port of Colón and other critical infrastructure along the Panama Canal.

- Alarmingly, China already owns, controls, or operates important sections of more than 40 major ports across Latin America, in many of which Chinese triads are also quite active.

- As a former SOUTHCOM Commander testified a few years back, China is the No.1 underwriter for the Mexican drug cartels, other criminal networks, and an array of despotic regimes. The Chinese government has been complicit in enabling the tens of billions of dollars in dirty money to be laundered through China.

- Colleagues, whether it is fentanyl, counterfeits, or money laundering for drug dealers and terrorists, if it harms the United States and the West, China will continue to use all of its national instruments to weaken us, while achieving Xi's 2049 strategic goals.

- In Venezuela, China has firmly supported the corrupt Maduro regime (even its sham elections and human rights abuses), not only because of its access and investments in the oil sector, but because it is a "strategic partner" to counter American influence in Latin America, as well as being an ally in its pocket at the United Nations, backing its territorial claims to Taiwan and South China Sea, and positioning China's military options in the event of war in the Pacific.

- If we look at Canada in recent years, it has become a crime convergence zone and forward operational hub for the world's most notorious crime groups and threat networks including the likes of Joaquín 'El Chapo' Guzmán and the Sinaloa cartel, Chinese drug kingpin Tse Chi Lop, Hezbollah Financier Altaf Khanani, and other bad actors,

- as well as professional enablers and drivers in the sectors of technology and maritime shipping (e.g., Vancouver port), and as a platform for financing global insecurity.

- For example, if you examine the so-called CCP police stations in North America, as certain investigative journalists have done in recent months, you have a nexus of PRC Intelligence Services operators converging with local Chinese triads in cities, often in the Fujian transnational crime networks.

- Such police stations are physically and mentally projecting Beijing's political power to influence the diaspora community politically.

    - They are connected to underground casinos, human trafficking and money laundering networks, and are connecting with other businesses to clandestinely fund influence and election interference.

    - China uses the triads as well to foment insecurity and illegality in democracies through diasporic communities. In fact, China's National Intelligence Law of 2017 calls on Chinese individuals, companies, and organizations to act as citizen spies for national security purposes.

Of course, another significant concern is China's growing network of facilities in Latin America related to its civilian space and satellite programs with defense capabilities.

- These ground stations have the potential to expand Beijing's global military surveillance network in the southern hemisphere and in areas close to the United States.

- Through economic coercion, China is also buying islands across the Caribbean (e.g., in Antigua and Barbuda), building special economic zones, and likely planning to use these commercial outposts for military purposes.

- In the U.S. Indo-Pacific Command (INDOPACOM) theater, PRC's efforts have destabilized the Solomon Islands, attempted to infiltrate Guam, undermined democracy in the Northern Mariana Islands and other Pacific Rim islands, and are seriously harming US relationships with those communities while isolating Taiwan diplomatically.

    - As democracy weakens and poor governance rises across these Pacific Rim Islands, China pounces and expands its influence through strategic corruption and their multi-polar agenda.

    - Moreover, as China infiltrates government institutions through coercive diplomacy, as reflected in the Security Pact with the Solomon Islands, Chinese law enforcement and military personnel can be called on to assist in "maintaining social order" or "protecting people's lives and property".

- Since the military took over in Burma/Myanmar, the PLA has worked with the Junta to build fentanyl factories to export precursors to Australia, Canada, New Zealand and anywhere else that they could get access.

- The money helped fund the PRC's malign influence and truth pollution to corrupt elections by using AI in Taiwan, Hong Kong, the Solomon Islands, Canada, in the U.S. and other countries according to the FBI.

- China has built military bases on several islands in the Spratly Islands, including air force facilities and other military installations to project power and shore up its vast territorial claims over virtually the entire South China Sea.

- These outpost bases and airfields are located on the three largest artificial islands: Mischief Reef, Subi Reef, and Fiery Cross. China has deployed a variety of weapons on these islands, including anti-ship and anti-aircraft missiles, radar, and fighter jets.

- The function of those islands is to expand the offensive capability of the PRC beyond their continental shores, and gain control over disputed territories.

- In fact, one can argue that China's Belt and Road Initiative (BRI) is intended to finance its economic, trade, and military expansion all around the world through its massive multi-trillion-dollar economic development assistance program.

    - However, as a result of the BRI loans (which some have called 'debt traps'), ruling kleptocrats in recipient countries have simply lined their pockets and padded their offshore accounts while enabling China to increase its influence and control of critical infrastructure across the developing world including ports, roads, pipelines, electrical power grids, mining, telecommunications, railroads, etc.

    - The licit trade channels and supply chains that the BRI has constructed have also created illicit pathways exploited by criminals, and the expansion of illicit economies globally.

    - In fact, the BRI global footprint tracks some of the biggest criminalized routes known for corruption, money laundering, and illicit trade. Further threat intelligence and data mapping can show overlays of illicit routes and criminal networks and how China helped to bridge a super highway of illicit economies globally, exporting forced labor practices, and violating human rights of both Chinese and local workers.

And of course, The Chinese triads are always behind these expansionist policies: Through the exploitation and controls of FTZs and ports and through the BRI, Chinese criminal syndicates are also able to expand illicit trade operations and unfair trade and business practices, moving contraband such as fentanyl, precursor chemicals for methamphetamines, counterfeit medicines and other illicit goods, as well as running illegal fishing and timber operations.

Iran

At the same time, Iran continues to threaten U.S. interests as it tries to erode U.S. influence in the Middle East, entrench its influence, and project power in neighboring states and in places such as Latin America.

- Iran's hybrid approach to warfare—using both conventional and unconventional warfare operations and a network of militant proxies -- enables Tehran to use strategic corruption and criminality to maintain strategic depth.

- Iran, through its Islamic Revolutionary Guards Corps (IRGC), is undertaking subversive active measures through its embassies, terrorist proxies, and criminal networks in Latin America to destabilize democracies and exercise political influence, penetrate illicit exert markets, and increase sway with corrupt ruling elites.

- Moreover, the Rabbani Network and Iranian Hezbollah Illicit Network are making billions of dollars from illicit trade and financing the information space to shape anti-democracy messages in the region in a manner that advances Iran's geopolitical goals.

- The Iranian collaboration with the Bolivarian Alliance and Bolivarian Joint Criminal Enterprise (BJCE) gives Iran more freedom of movement; and

- leverage access in the region as it allies with Bolivia, Cuba, Nicaragua, Venezuela, and other countries to export their malign influence, intelligence operations, criminal activities, and threat convergence strategies that are often coordinated with China and Russia.

- Iran uses friendly Latin American countries as strategic staging grounds to foment chaos and insecurity in the region, and to advance it operational platforms and disinformation campaigns against the United States and its democratic allies.

- Iran's primary military engagement with its Bolivarian allies has been through supporting a military doctrine that eradicates any vestige of U.S. military influence in the region and replaces it with an asymmetrical or hybrid warfare.

- The Iran Hezbollah Threat Network (IHTN) provides the means to wage that warfare for Iran and its global allies, and as a fundraising vehicle to finance terrorist attacks internationally.

- Iran established its beachhead in Latin America through Venezuela. Hugo Chávez, the late authoritarian leader, opened crucial doors for IHTN operatives and surrogates in the hemisphere. Chávez often invoked and used similar political rhetoric as Iran to describe the United States (e.g., "Great Satan").

- The strategic alliance begun with Chávez and then Iranian prime minister Mahmoud Ahmadinejad blossomed into a strategic military, intelligence, and economic alliance. With Venezuela's support, Iran was able to expand its clandestine operations and malign influence activities across Latin America.

- Iran has leveraged the IHTN as a strategic proxy to collect intelligence in Latin America against the United States, destabilize its regional interests, and engage in fund-raising across diasporic Shi'ia communities in the TBA in South America, and beyond.

- This includes using adaptive adversaries such as terrorists, insurgents, and criminal networks to engage in asymmetrical warfare, and leveraging "sleeper cells" to infiltrate governments and carry out attacks in the TBA, and beyond. IHTN activities are further aided by professional facilitators, corruption, organized crime, political violence and instigated chaos.

In a nutshell: through a confluence of geo-security interests, China, Russia, and Iran continue to strengthen intelligence and military ties to weaken democratic institutions, expand illicit economies, and bolster autocratic governance around the world.

Threat Convergence: A Threat Multiplier

In many parts of the world, a perfect storm is brewing.

As mentioned earlier, as kleptocrats, criminals, terrorists, and other bad actors and threat networks work in certain geographic coordinates and points in time across illicit spaces,

- they are all increasing corruption and criminality, and thus, making it easier for authoritarian states to exploit further such gray zones to advance their national and joint interests.

- Their motto seems to be "the more the merrier" as they work to propel converging forces to destabilize, divide, and conquer markets, democracies, and strategic lands and territories.

Often authoritarian regimes strictly control outreach and foreign policy.

- Integrating criminal proxies brings speed, intelligence, revenue, and chaos.

- For example, the PRC runs fentanyl campaigns that fund bribes to political groups, influence operations, and integrate criminal gangs with paramilitary groups to buy political support, economic advantage, and target dissidents in that nation, all while making a profit.

- Adversaries and competitors are turning the West's economic, political, legal, and social systems against their own people and governments.

In summary: State-backed strategic corruption and criminality enable authoritarian-led adversaries to:

- gain a foothold in political institutions;

- finance local militant groups, criminals or terror cells to ignite instability and throw a coup;

- to enrich themselves for personal gain; and

- to fund greater chaos and insecurity through active geo-strategic corruption such as China, Iran, North Korea, Russia, and others, are undertaking in many parts of the world.

Again, such active measures and malign influence work to not only weaken Western democracies, but to fulfill their shared ambition of creating a multipolar world order, untethered to the norms of democratic governance and rule of law.

- A world of threat convergence is a confluence of autocrats, organized crime, and criminalized states expanding and exploiting illicit economies globally by orders of magnitude, in ways democratic governments are struggling to understand, map and confront.

Authoritarian regimes, like South Sudan, survive by stoking instability and conflict within their nation to stay in power and more easily sell natural resources for personal gain.

- In the past, these regimes would have destabilized and collapsed; but by partnering with criminal groups and threat actor militia proxies,

- these regimes are able to more cruelly oppress public opposition and remain in power while the region struggles with the refugees and violence spreading into their nations.

Special Action Task Forces: Prosecuting Authoritarian Subversion and Strategic Corruption and Criminality

In today's great power competition world, we must innovate.

Akin to the modus operandi of transnational criminal organizations, China, Russia, and other illicit threat networks have perfected the strategic dark art of acting first and faster than countervailing police and security forces when undertaking subversive activities.

Our response should be anticipatory and dynamic: Action beats reaction.

This entails more robust threat horizon measures including:

- integrating threat intelligence overlays and multi-dimensional capabilities to counter threat convergence in national strategies so that we can better anticipate changing threat environments, and protect U.S. national security interests from TCOs and illicit threat networks.

We also need to be sharing threat intelligence in a timely manner to mitigate harms.

Unfortunately, across almost all of today's illicit industries, we are losing the war against both illicit threat networks and state-sponsored criminality and corruption.

- The problem is exacerbated because governments are not making these threats a top national security priority,

- Efforts to combat these adversaries are thwarted by outdated intelligence analysis,

- the lack of understanding of the scale of these challenges;

- speed, connivance, and use of sophisticated technologies by criminals and malign state actors; and finally

- failure to make the requisite adaptations and investments necessary to effectively counter such transnational threats or incentivizing fragile governments on the brink of being captured by China, Russia, and Iran.

And as clearly articulated earlier, the NSC needs to build and manage whole-of-government and whole-of-society campaigns that respond to adversary and competitor nations' trade, military and criminal actions.

- A unified whole-of-system response is needed.

- Additionally, these campaigns need Agencies to update intelligence requirements, analysis expectations, and use targeting that includes all aspects of our adversaries and competitors.

- Essentially a PMESII-PT framework is needed to optimally analyze operational hybrid warfare environments, and dark shadowverse of criminality and corruption.

  [PMESII-PT: stands for Political, Military, Economic, Social, Information, Infrastructure, Physical environment, and Time.]

- Only targeting military threats without removing the economic backing and political and social malign influence allows the threat to rebuild and expand.

One key enhancement of our ability to combat these threats would be to create an inter-agency or DoD Irregular Warfare Task Force to Counter Malign Influence and Strategic Transnational Illicit and Corrupt vectors (IWTF: C-MISTIC) by China, Iran, Russia, and other authoritarian states, in fragile states and gray zones.

(White Paper attached: Special Action Teams)

- China, Iran, and Russia are overwhelming the rule-of-law systems in many jurisdictions where bribery and criminality thrive, including by corrupting, softening up, and subverting key governance, political, law enforcement, and security systems that result in state capture, losing committed democracies and allied partners that work with the United States to counter authoritarianism.

- Building on DOJ's national rapid response strike forces in the United States that examine numerous corruption and fraud cases, the DOD IWTF: C-MISTIC would be invited to

deploy to partner nations' jurisdictions to investigate and prosecute webs of foreign bribery, strategic corruption, and cross-border criminality, and to provide expertise and capacities to conduct complex cases.

- These special action teams could respond to adversary operations by reinforcing the rule of law in U.S. territories and partner nations and assisting in investigations and prosecutions, for example in Pacific Rim Islands.

- Such a Task Force could be supplemented with specialized Guard and Reservists, who, as civilians, are experienced criminal investigators, attorneys, prosecutors, and federal judges who support the courts.

- A Task Force could also provide support to Intelligence and Enforcement. It would help analyze data and map illicit networks and dirty money flows that can be used as evidence to warrant further cross-border sharing of information, investigations and prosecutions of bad actors and disruption of malign influence operations.

In closing: Today the international law enforcement and security communities are under even more pressure, often out-resourced, outmanned, and sometimes, out-gunned.

- At this point in time, security forces have become largely reactionary instead of proactively working to mitigate the risks and threats posed by organized crime and illicit threat networks.

Currently, the military, intelligence, international law enforcement and security communities are under enormous pressure to find solutions.

- Often their efforts are over siloed, and out-resourced.

- Integrating military, economic and criminal analysis, targeting and effects removes 80 percent of the problem,

- but more importantly, cuts off the fuel that the networks use to grow and sustain their efforts.

- This allows political and social reforms to then combat the malign influence and restabilize our partner nations' governance and civil societies.

Without more anticipatory and innovative IW frameworks to counter strategic corruption and criminality, we may not meet these challenging threats.

- To win, we must effectively counter our adversaries and competitors with more innovative resource-sustained IW and anti-crime tools and capabilities including realizing and fully capitalizing new Marshall Fund Initiatives (e.g., G7's 2022 $600 billion proposal) to Counter Authoritarian-Financed Strategic Corruption and Criminality.

- We must outfox and react faster to the deviant machinations of adversaries operating in the gray zones.

- We need a new baseline understanding that integrates global transnational criminal structures into our collection, analysis, targeting and operations to cut the support and logistics of our adversaries and competitors.

- It's no longer one or another agency's problem, it's everyone's problem and we need a solution before we are on the run.

Unless we up our game and get ahead with the required political will, resources, and energies needed to push these security boulders up the hill, the battle against many of today's cross-border threat convergence harms will remain a Sisyphean task.

We must keep the flames of democracy burning in the face of rising authoritarianism and strategic corruption.

Thank you.