GLOBAL GUARDIAN

WORLDWIDE THREAT ASSESSMENT

MARCH 2023

GLOBALGUARDIAN.COM 703.566.9463 INFO@GLOBALGUARDIAN.COM

TABLE OF CONTENTS

Global Guardian publishes an annual overview of recent global security developments. This year, Global Guardian's Intelligence Analysts assess two key second and third-order effects of the War in Ukraine and two areas of mounting geopolitical tension in East Asia. The report looks forward, assessing trends within the next 12-36 months. Ultimately, the goal of this report is to evaluate emerging risks and their impacts with a focus on how they will shape future safety and security concerns for global businesses and international travelers.

To meet these new challenges, Global Guardian offers an integrated suite of best-in-class security services that help clients identify and mitigate the risks associated with travel and conducting business both overseas and domestically. These services include personnel tracking, emergency response, security and transportation support, intelligence and due diligence, medical support and evacuation, emergency and custom aviation, cyber security, and video surveillance monitoring.

Global Guardian seamlessly integrates and delivers these capabilities under the close guidance of its 24/7 Security Operations Center.

THE POST-SOVIET SPACE IN DISARRAY

As Russian power is sapped in Ukraine, countries throughout the post-soviet space, traditionally reliant on the Kremlin for security, are now left without a protector. The Azerbaijan-Armenia conflict, based on ethnic grievances and Soviet- era borders, is a bellwether of what may be in store for Central Asia, where the Kremlin's waning influence has led to an expanding Chinese security presence.

But Beijing's role as the new regional security provider may be more harmful than helpful due to its deep unpopularity in parts of Central Asia. Between China's unpopularity and lack of legitimacy, and Russia's preoccupation with Ukraine, Central Asia lacks a cohesive security architecture. As the regional order decays, local disputes could spiral into wider conflicts with serious implications for global energy and mineral supplies as well as regional stability.

THE SUBJUGATED STEPPE

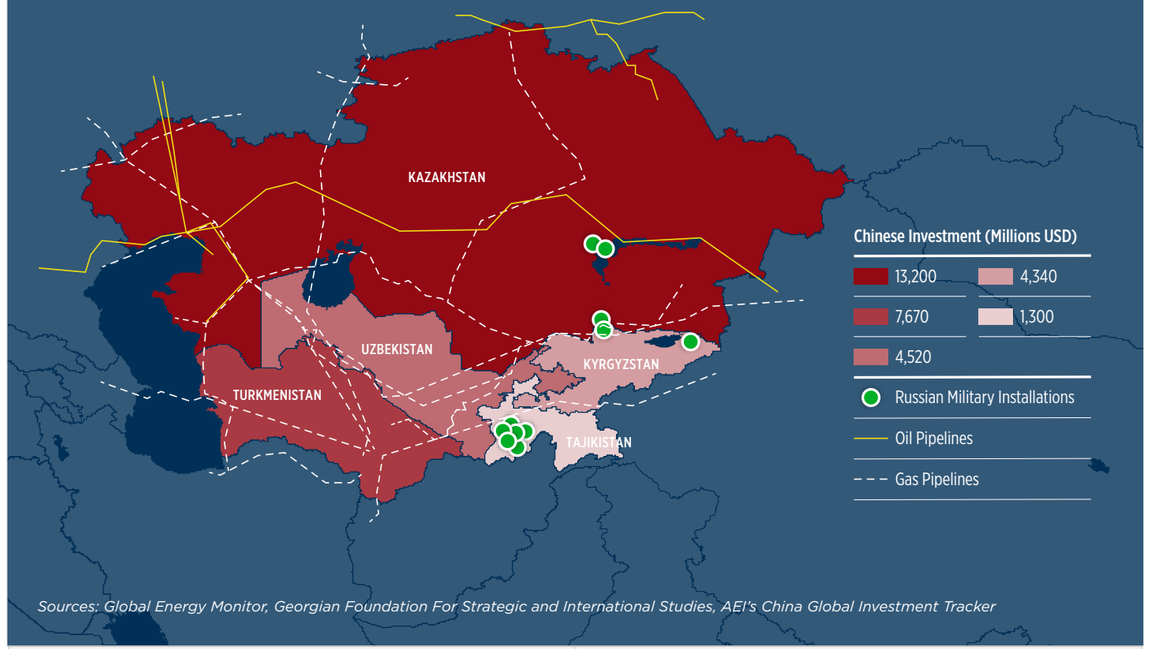
Long ruled by the Russian Empire as a singular entity called Turkestan, the five states of Central Asia – Turkmenistan, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan – acquired their current political borders under Soviet leader Vladimir Lenin. These artificial lines split tribes, ethnic groups, and other identities that transcend the current political boundaries. Following the dissolution of the Soviet Union in 1991, the leaders of the newly independent states continued to look to Moscow to provide order and buttress their largely autocratic regimes.

But in 2013, the Central Asian republics began to increase their financial reliance on Beijing, owing to China's Belt and Road Initiative (BRI). While China's gain appears to come at Russia's expense, friction between the two autocracies takes a back seat to their shared struggle against the United States (U.S.)-led liberal international order. Consequently, Russia and China have operated with an implicit geopolitical division of labor in their mutual backyard for the past decade: China acts as the banker and Russia as the sheriff (see Figure 1).

The arrangement returned dividends for both countries. The Russian and Central Asian economies are highly integrated, so Moscow has benefited greatly from Beijing's regional investments. China has enjoyed the stability provided by Russian security leadership in the countries that border its own restive Xinjiang province. The partnership functioned in part because neither Moscow nor Beijing was inclined to replace the other's contribution. But now, in the absence of a viable sheriff, the post-Soviet space could become increasingly violent.

THE BANKER AND SHERIFF:
RUSSIAN AND CHINESE INTERESTS IN CENTRAL ASIA

Figure 1



Sources: Global Energy Monitor, Georgian Foundation For Strategic and International Studies, AEI's China Global Investment Tracker

Russia	China

• Benefits from immense – but decreasing – soft power from the Soviet educational legacy and the seven million ethnic Russians living in Central Asia.
• Enjoys double-digit leads over China in approval polls.
• Increasingly reliant on trade with Central Asian countries to circumvent Western sanctions and support the war effort.
• The Russian-led CSTO routinely holds joint counterterrorism drills with Kyrgyzstan and Tajikistan near China's border with Afghanistan.
• Russian intelligence spearheaded an investigation into the 2016 bombing of the Chinese embassy in Bishkek, Kyrgyzstan.
	• The region is central to China's Belt and Road Initiative.
	  • Owns more than USD $40 billion of Central Asian sovereign debt and has deployed USD $40 billion in loans and investments.
	• Committed to securing Xinjiang province from "Extremism, Terrorism, and Separatism."
	  • Xinjiang is home to millions of Turkic people with linguistic, cultural, and religious ties to populations in Central Asia.
	• Increasingly reliant on Central Asian energy as it shifts away from coal.
	  • Turkmenistani gas accounted for 50% of China's piped natural gas imports in 2022.
	  • Kazakhstani uranium accounted for 48% of China's uranium imports in 2021.

CANARY IN THE CAUCUSES

Today, Russia's absence in its former dominions is felt most acutely in the Caucuses where Azerbaijan is enforcing an effective blockade of Nagorno Karabakh – a de facto Armenian enclave – despite the presence there of more than 2,000 Russian peacekeepers. Armenia, a member of the Russian-led CSTO, relies on Russia for protection and armament, but as Moscow struggles to maintain its territory in Ukraine, neither are forthcoming. Moscow's inability to play peacemaker has led not only to a resumption of perennial hostilities between these two former Soviet republics, but to increased involvement by outside actors such as Türkiye and Iran, whose influence in the region has historically been checked by Russian power.

The conflict between Armenia and Azerbaijan shares more than a few parallels with potential conflicts in Central Asia. In both Central Asia and the Caucuses, former Soviet republics tend to be unstable, have underlying ethnic tensions, and are reliant on Moscow. The conflict in the Caucuses today may presage what lurks in Central Asia tomorrow.

FUTURE RISKS IN CENTRAL ASIA

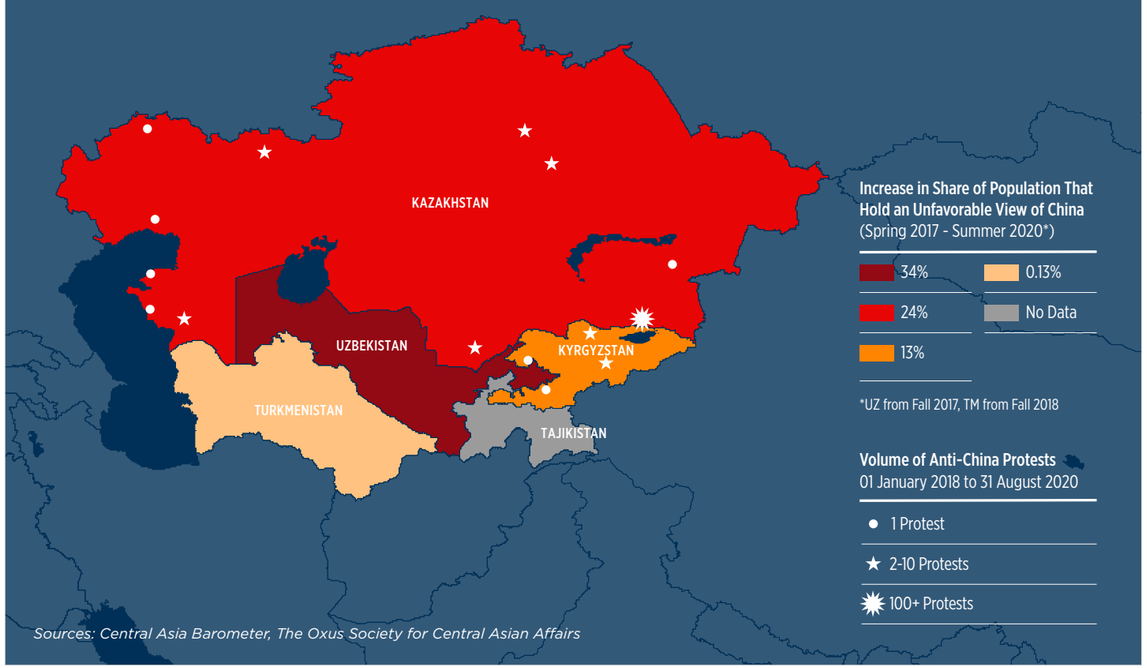
Civil Unrest

Case | Kazakhstan: In September 2021, protests began in the Kazakhstani city of Zhanaozen in response to rumors of new Chinese factory construction. As the unrest spread to Almaty and Astana, the demonstrators' list of anti-China grievances grew to include land purchases, environmental concerns, taking local jobs, and human rights abuses of the roughly 1.5 million ethnic Kazakhs living in Xinjiang (see Figure 2). Less than a year later, in January 2022, the Kazakhstani government of President Tokaev removed price caps on natural gas, setting off ten days of violent protests. The demonstrations quickly escalated into fatal clashes between protestors and police as unrest again spread from Zhanaozen to Almaty and Astana. Ultimately, the presence of CSTO troops – including a contingent of 3,000 Russian paratroopers – proved critical to the restoration of order.

Analysis: Russia was able to quell the Kazakhstani protests largely owing to its popularity with the local population. Notably, the anti-regime protests did not become anti-Russia protests after Moscow's intervention. While Russia's public perception has undoubtedly been damaged by its invasion of Ukraine, it is still substantially more popular than China in the region, where the percentage of people with an unfavorable view of China has risen roughly 25% since 2017.

ANTI-CHINA SENTIMENT IN CENTRAL ASIA

Figure 2



Sources: Central Asia Barometer, The Oxus Society for Central Asian Affairs

> "Faced with a zero-sum contest for water, unclear borders, and a habit of seeking legitimacy through conflict, the countries of the Ferghana Valley (Uzbekistan, Tajikistan, and Kyrgyzstan) are sliding towards inter-state conflict."

China's decline in popularity in Kazakhstan is tied to its increasing presence in the country. This trend suggests that even a multilateral Chinese intervention in Kazakhstan on the regime's behalf could drastically reduce the popularity of both China and the regime. Taken together, the protests of 2020 and 2021 demonstrate the potential for widespread economic dissatisfaction to combine with ethno-religious grievances culminating in unrest that is simultaneously anti-Chinese and anti-regime. These underlying factors are present to varying extents throughout Central Asia. Paradoxically, as China cools the pace of its BRI investments due to its own economic woes, the medium-term economic outlook for the region worsens, which could drive unrest.

Interstate Conflict

Case | Kyrgyzstani-Tajikistan Border Clash: In September 2022, a localized border conflict over access to resources escalated into a skirmish that left roughly 100 dead, 200 wounded, and more than 130,000 people internally displaced. The clash featured the use of heavy weapons sourced from India and Iran, as well as advanced drones from Türkiye. As the violence escalated, both the Kyrgyzstani and Tajikistani presidents, in addition to their Russian and Chinese counterparts, were present at the Shanghai Cooperation Organization (SCO) summit in Samarkand, Uzbekistan, a scant 200 miles away from the fighting. Yet, neither President Xi nor President Putin addressed the violence at the summit, indicating an unwillingness to involve themselves in cross-border conflicts.

Analysis: Both Kyrgyzstani President Sadyr Japarov and Tajikistani President Emomali Rahmon routinely use border conflicts to shore up domestic legitimacy. Leveraging border conflicts for legitimacy not only paves the way for internal regime crises to escalate into regional crises, but these political tactics virtually guarantee that similar conflicts will occur in the future. As Russian support for Central Asian regimes decreases, local leadership will face increasing pressure to appeal to nationalism and traditional ethnic rivalries to maintain power. This danger is amplified by thousands of kilometers of disputed borders, myriad ethnic enclaves, and most significantly, perennial disputes over access to water.

Over the past decade there have been more than 150 border skirmishes between Tajikistan and Kyrgyzstan, with a majority involving shared water sources. The trend has grim implications going forward. Due to a combination of climate change and the expansion of water-intensive agricultural and mining operations, Central Asia is rapidly drying. Faced with a zero-sum contest for water, unclear borders, and a habit of seeking legitimacy through conflict, the countries of the Ferghana Valley (Uzbekistan, Tajikistan, and Kyrgyzstan) are sliding towards inter-state conflict. With Russia and China on the sidelines, there is no clear hegemon to force de-escalation.

TAKEAWAYS

The Soviet Union purposefully shaped its periphery to be unstable and reliant on the Kremlin. Now, as Russia's attention and might is focused on Ukraine, the traditional security architecture that stabilized the post-Soviet space is beginning to crumble. In the Caucuses, the Russian-brokered peace is unraveling. In Central Asia, regime insecurity and border skirmishes will soon threaten to escalate into regional conflicts where other regional powers are actively arming the belligerents. Beijing is starting to fill the void left by Moscow's absence, but lacking Russia's legitimacy, a future Chinese security presence will not ameliorate the coming crises, it will exacerbate them.

CHIP WARS: THE GEOPOLITICS OF SEMICONDUCTORS

The global semiconductor supply chain has emerged as one of the key theaters of geopolitical competition. With its dominant position in the semiconductor supply chain, the United States (U.S.) is leveraging sanctions and export controls on its geopolitical adversaries – Russia and China – to great effect. However, with semiconductor production concentrated in East Asia – China's backyard – Beijing has the ability to disrupt the entire value chain. In the battle to achieve semiconductor self-sufficiency, both control over the fourth industrial revolution and the sovereignty of Taiwan are at stake.

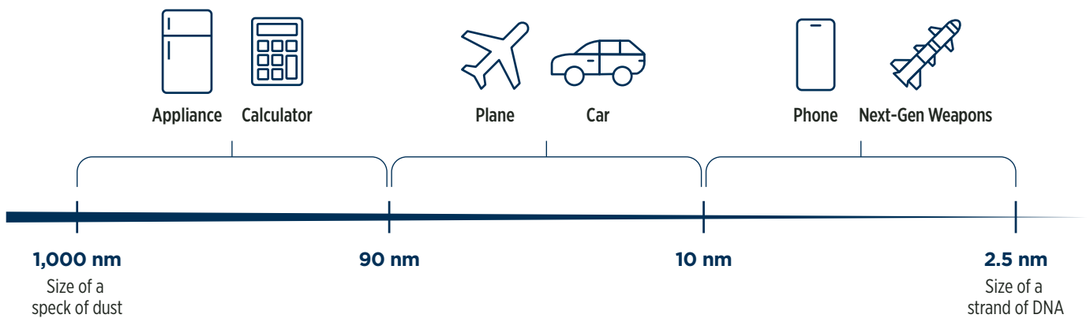
Semiconductors, commonly known as microchips, are a series of microscopic transistors sitting on silicon wafers that regulate the flow of electricity in circuitry. Chips are essential to all electronic devices. The more transistors, the more processes an electronic device can carry out, and the smaller the nodes, the more chips can fit inside a particular piece of equipment. But microchips aren't just essential for consumer goods; cutting-edge semiconductors are vital for both current and future military technologies (see Figure 3).

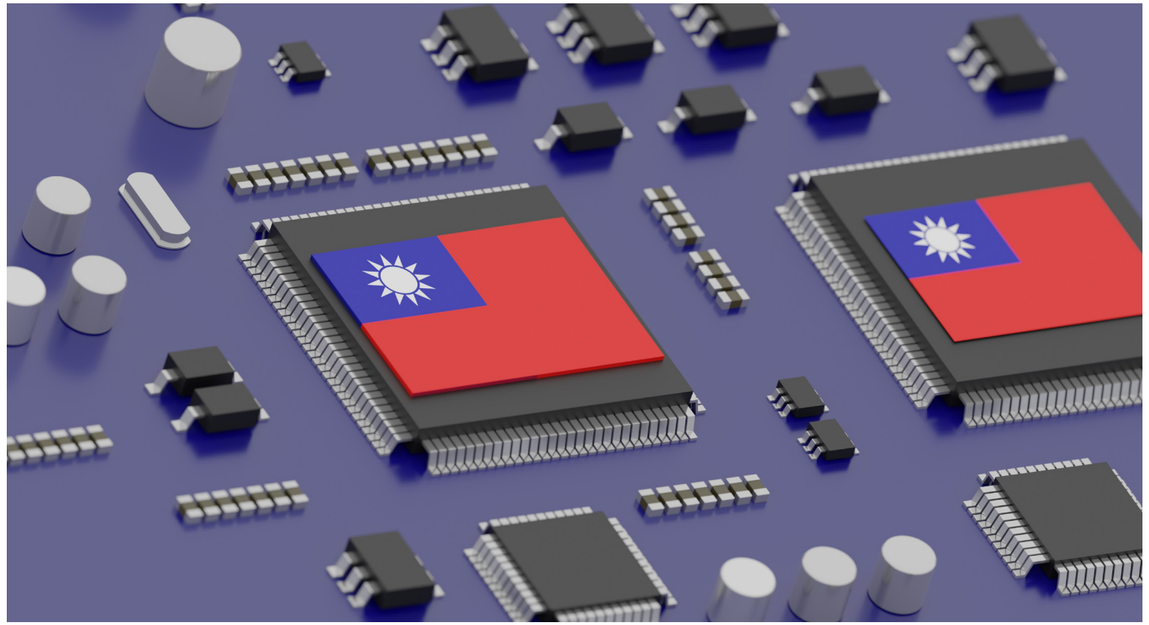
GLOBALIZATION EPITOMIZED

The semiconductor value chain is complex and highly globalized. It involves five steps: research & development (R&D), design, manufacturing, assembly, testing and packaging (ATP), and distribution. Owing to the complexity of the process, there are only four integrated device manufacturers (IMDs) - chipmakers that are vertically integrated. The IMDs include Intel and Micron Technologies based in the U.S. and Samsung and SK Hynix in South Korea. But these IDM companies still have offshore assets and rely on raw materials and machinery from other companies based in different countries. Most of the industry follows the fabless-foundry model which outsources segments of the value chain to firms in Taiwan, China, and Singapore to lower production costs.

In broad terms, the silicon comes from China, the neon gas needed to operate deep ultraviolet (DUV) lithography machines comes from Russia and Ukraine, R&D and design occur in the U.S., the silicon wafer cutting equipment comes from Japan, and the lithography machines – the equipment that cuts the tiny transistors – are made in the Netherlands by the firm ASML with parts from Japan and Germany (see Figure 4). The manufacturing (fabrication) includes cutting silicon into wafers and printing circuit patterns onto the polished wafer surfaces (microlithography) and is overwhelmingly concentrated in East Asia. Currently, 85% of the most advanced microchips – 5 nanometers (nm) and below – are fabricated in Taiwan and 15% in South Korea. Meanwhile, 65% of legacy (16 nm and above) logic chips are fabricated in China and Taiwan.

TRANSISTOR NODE SIZES AND APPLICATIONS Figure 3





THE "SILICON SHIELD"

Taiwan's centrality in the semiconductor value chain and its geographic location have granted Taipei protection. Over the years, Taiwan established itself as the center of global chip fabrication, now controlling 66% of the semiconductor foundry market. Taiwan's semiconductor manufacturing capacity is indispensable to both China and the U.S., thereby giving it a "Silicon Shield" – neither the U.S. nor China has the capability or capacity to replace Taiwan. The Taiwan Strait, - which separates Taiwan from mainland China - is a maritime chokepoint traversed by 48% of the global container fleet. Thus the U.S. protects Taiwan, and China is disincentivized from invading it. But this dynamic is changing; chinks in this shield are starting to grow.

Container shipping logistics issues in 2020-2021 awakened both business leaders and governments to the fragility of East Asia-centric supply chains. The just-in-time inventory model, especially in the semiconductor space, was proven to be untenable, especially for goods vital to national security. In total, pandemic-related supply issues took away an estimated quarter-trillion dollars of U.S. GDP growth in 2021. The resulting inflationary pressure, tangible scarcity, and foreign dependence were too large for politicians to ignore.

BATTLE FOR SEMICONDUCTOR SOVEREIGNTY

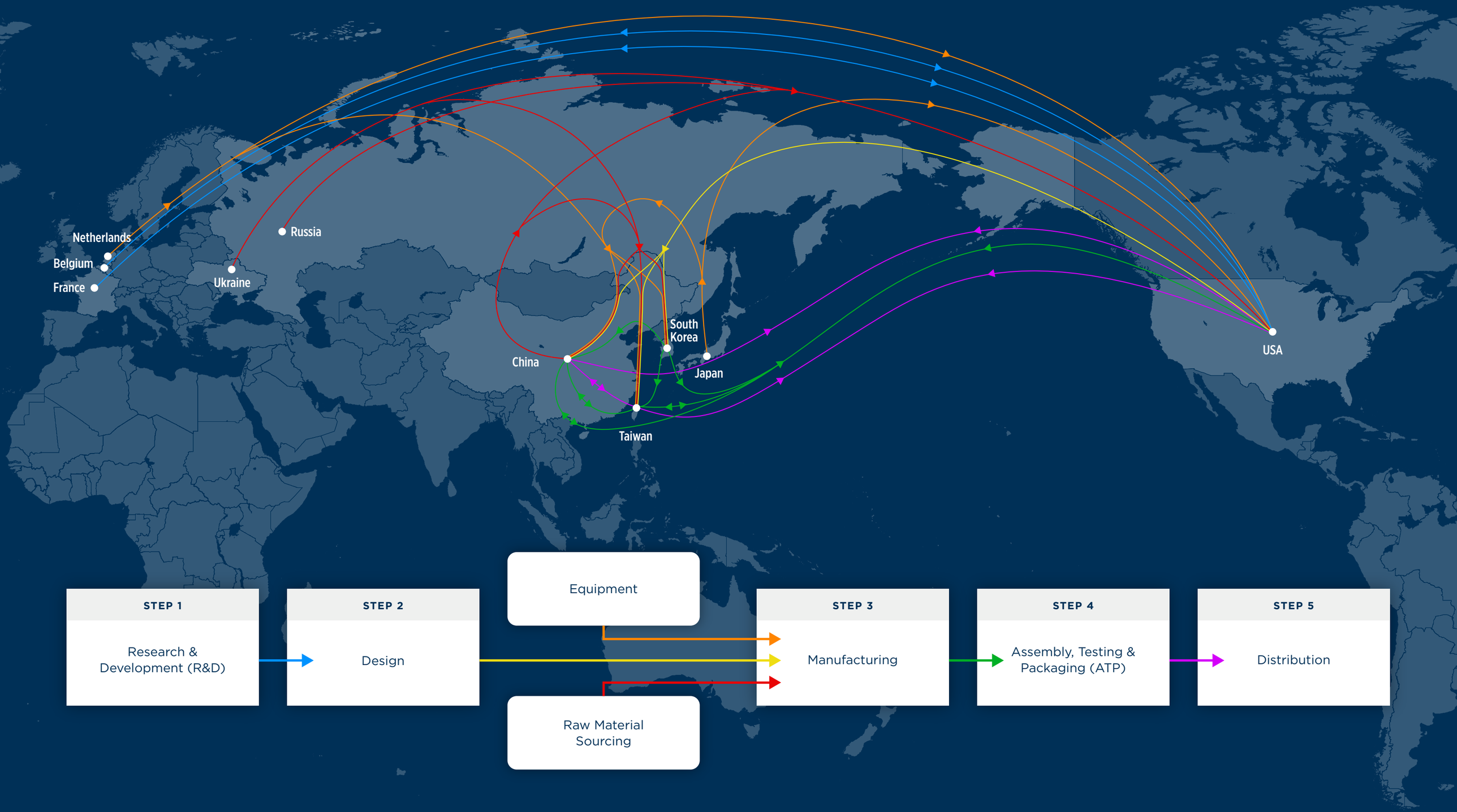
Reshoring the semiconductor supply chain has taken a front seat in American government policy. In the 1960s, semiconductors were designed, manufactured, and assembled entirely in the U.S. but over time, outsourcing manufacturing and assembly became more economical. Currently, the U.S. only produces 12% of the world's semiconductors. But this is about to change.

TSMC, Samsung, and Intel are now building advanced chip fabrication plants in America set to go online between 2024 and 2026. Furthermore, U.S. Congress passed the CHIPS Act in 2022, which directs USD $280 billion in federal spending on the semiconductor value chain over the next decade, earmarking USD $200 billion for R&D and USD $52.7 billion for semiconductor manufacturing. By the start of the next decade, the U.S. will no longer be dependent on chips manufactured in Taiwan.

Meanwhile, China currently accounts for about 60% of global demand for semiconductors but only produces some 13% of global supply. To this end, part of China's Made in China 2025 five-year plan is to secure dominance in high-tech sectors and become 70% self-sufficient in semiconductor production. China has created investment funds to prop up its domestic value chain, investing over USD $220 billion in subsidies. Additionally, China has become the world's largest importer of semiconductor manufacturing equipment over the last two years.

THE SEMICONDUCTOR VALUE CHAIN

Figure 4



EXPORT CONTROLS & SANCTIONS ON CHINESE CHIP MAKING

Figure 5

MAY 2019 Huawei added to U.S. export blacklist

JUN 2019 China's SMIC delisted from the New York Stock Exchange

JAN 2020 U.S. pressures Dutch government to block ASML from selling extreme ultraviolet lithography (EUV) machines to China

JAN 2021 U.S revokes Intel's export license to sell chips to Huawei

JUL 2022 U.S bans the export of all equipment involved in fabricating chips of 14 nanometers or smaller

JUL 2022 U.S. bans export of electronics design automation (EDA) software for China's advanced chipmaking

AUG 2022 U.S. bans export of high-performance GPU chips to China

OCT 2022 U.S blacklists exports to 31 Chinese chipmaking companies

U.S restricts American citizens and companies from providing direct or indirect support to Chinese companies involved in fabricating chips of 18 nanometers or smaller

JAN 2023 Japan and the Netherlands agree to export controls on semiconductor equipment to China

But China still fundamentally lacks the knowledge to produce cutting-edge chips. It lags behind in chip design software and does not produce its own advanced semiconductor manufacturing equipment (SME). Further, it has a human capital deficit and remains dependent on foreign talent for technical know-how and has used high salaries to aggressively poach international employees from top firms. These deficiencies have put China five to eight years behind its competitors in the chip race. All the while, two consecutive U.S. administrations have tried to maintain this lead through sanctions (see Figure 5).

JETTISONING CHINA

In October 2022, the Biden Administration introduced sweeping new restrictions on the export of semiconductor chips to China. U.S. strategy has now shifted from delay – buying time as it builds its own domestic semiconductor production by slowing China's technological progress – to destruction. The new export controls make it illegal to sell or service equipment and technology needed to manufacture chips at and below the 18 nm size to any Chinese company without a license, thereby preventing China from developing and accessing advanced computing hardware. The sanctions apply to any company employing American technology to create products and prevents American citizens from working in the Chinese semiconductor value chain. Not only do these new rules kneecap China's technological progress, but they also effectively degrade China's current ability to obtain or produce mid-range semiconductors.

In January 2023, the Netherlands and Japan joined the U.S. with export controls targeting China. There are almost no alternatives to the design, software, and equipment emanating from the U.S., Japan, and the Netherlands. Even more damaging than the export restrictions themselves is the sealing off of China from Western know-how. More than 40 American executives at Chinese semiconductor firms are now faced with the choice of resignation or renouncing their U.S. citizenship, and Americans working in other parts of the value chain have been ordered to stop interacting with Chinese firms. For example, key American executives at China's leading SME maker Piotech, including its CEO, resigned. It is unclear how China will be able to make up for this knowledge gap.

While the U.S. has correctly assessed that its control over critical parts of the semiconductor value chain can be levered against its rivals, the U.S. is not the only power with the ability to exert control over elements of the microchip ecosystem.

THE CHIPS CHINA HOLDS

So far, Beijing's response to the new U.S.-led export control regime has been inward. In December 2022, China began working on a USD $143 billion support package for its semiconductor industry with a focus on subsidizing the purchases of Chinese-made semiconductor equipment. With China's new pro-Xi political leadership firmly in place after the March 2023 National People's Congress, President Xi may now have the will and power to push through more aggressive retaliation against the U.S. and American business interests. In the past, China has employed narrow tit-for-tat measures, but Beijing has three major vectors through which it can retaliate against U.S.-led efforts to prevent China from achieving semiconductor sovereignty.

2021 Anti-Foreign Sanctions Law: This law gives the Chinese government a legal tool to respond to foreign sanctions with its own counter-sanctions, namely, the blacklisting of individuals and companies doing business in China. Sanctioned businesses or individuals can be blacklisted or deported, banned from financial transactions with Chinese institutions or entities, and have their assets in China seized or frozen.

Raw Materials: China leads the world in both silicon and gallium production (needed for chips) accounting for 68% and 97% of global reserves and production, respectively. China also has a near monopoly on rare earth metal processing, with the U.S. importing 80% of these materials from China. By banning or limiting the export of these materials, Beijing could throttle access to these resources, creating catastrophic short-term supply disruptions for chipmakers and in the numerous high-tech industries that use rare earths — telecommunications, electric vehicles, renewables, batteries, and defense. China's monopoly on key aspects of the solar energy value chain could also be weaponized to prevent the U.S. from achieving its climate goals.

Transportation Disruptions: The vicissitudes of demand for semiconductors were only part of the pandemic supply chain issue. China's closing of its ports and the congestion associated with reopening them was a major factor in the 2020-2021 delivery delays. Policy makers in Beijing now understand that they can cause bottlenecks in the supply chains for many products, including microchips. This leverage was on full display when China conducted military drills around Taiwan following U.S. Speaker Pelosi's trip to Taipei in 2022, effectively blockading the island.

As Sino-American relations continue to worsen, export controls could expand into blanket sanctions on the entirety of China's semiconductor industry, potentially removing China's ability to import chips from Taiwan and South Korea. Should this situation arise, China's window for preventing the U.S. from securing its own semiconductor sovereignty will close by the end of the decade, coinciding with U.S. military estimates of when China will be ready to invade Taiwan. President Xi may decide if China isn't getting its much-needed chips from its own backyard, then no one else will. Short of an invasion, China could employ its maritime militia or other non-military forces to harass and interdict shipping to and from Taiwan.

UKRAINE VS TAIWAN

While so far, military aid to Ukraine has not come at the expense of Taiwan's defense. Most arms shipments to Ukraine have come directly from U.S. stockpiles, bypassing the complex foreign military sales process. But should the war persist, Taiwan and Ukraine will soon begin to compete over weapon systems (Javelin and Stinger missiles, High Mobility Artillery Rocket Systems, Army Tactical Missile Systems, Harpoon missiles) partially due to the scarcity of the chips that go into them. At present, there is a USD $18.7 billion backlog of weapons destined for Taiwan, mainly stemming from issues in the defense industrial base and the over bureaucratization of the foreign military sales process. As the war drags on, the U.S. will have to selectively prioritize which shipments to fulfill first. Any disruptions to the semiconductor or electronic device supply chain more broadly will inevitably create a scarcity situation.

TAKEAWAYS

Semiconductor sanctions are proving to be one of the most powerful levers in in the U.S. foreign policy playbook but paradoxically, their efficacy may increase the likelihood of a geopolitical showdown between the U.S. and China. While efforts are being made to fortify the highly globalized semiconductor supply chain, the process may take a decade. Until then, the fragility of the current supply chain may pose serious risks to the global economy and the loss of the Chinese market will harm Western chip firms. After all, if China cannot import chips from Taiwan or build its own chips using U.S. tech, what is preventing Beijing from "reunifying" with Taiwan? The longer Beijing waits, the more leverage it loses as the U.S. and its partners diversify their supply chains away from China.

AGE OF THE AVBIED

Until recently, advanced militaries and their export partners were the sole operators of modern drone technology. But with technological advances – improvements in range, speed, payload, control and coordination, and propulsion – and most importantly, sharp declines in price, commercially available drones (CADs) have become ubiquitous. Tools once reserved for powerful state militaries are now in the hands of non-state actors. Just as military drones' primary purpose shifted from intelligence, surveillance, and reconnaissance (ISR) to also becoming weapon delivery platforms, commercial drones are now being used for this end. The extensive use of off-the-shelf drones as delivery vehicles for improvised explosive devices (IEDs) on both sides of the Ukraine conflict will inspire bad actors to employ drones as a force multiplier. In the coming years, CADs will become a weapon of choice for nefarious non-state actors, including Islamic extremists, far-right groups, ecoterrorists, transnational criminal groups, street gangs, and aggrieved individuals alike.

A VERSATILE PLATFORM

There are two ways in which CADs can be leveraged as a delivery platform for IEDs: directly and indirectly. Direct aerial vehicle-borne improvised explosive devices (AVBIEDs) are kamikaze drones, whereby CADs are rigged with explosives designed to detonate on impact. The direct AVBIED is the analog for advanced militaries' loitering munitions, which are in essence smaller, slower, cheaper, and less detectable cruise missiles. Indirect AVBIEDs are CADs that act as a platform to deliver another weapon and are designed for reuse. They are used to drop grenades and can even have weapons mounted on them, including small arms or aerosolized spraying devices.

THE UKRAINE EFFECT

There is nothing new under the sun. Successful tactics, techniques, and procedures (TTPs) used on one battlefield are always studied and assessed by other interested actors. Non-state actors, including terror groups, have demonstrated their aptitude for sharing information and emulating new successful TTPs. For example, in the 2010s, car ramming, a tactic pioneered by lone wolf Palestinian terrorists, due to its accessibility and its difficulty to counter, was then emulated across Western Europe to devastating effect.

Following the onset of the war in Ukraine, footage of Ukrainian forces using readily available commercial drones to drop grenades into Russian vehicles and trenches began to circulate across social media, boosting the profile of this mode of attack (see Figure 6). While sophisticated non-state actors have already employed weaponized CADs in battle, we have yet to see successful AVBIED attacks on civilians outside of a warzone. But this is not for a lack of trying. Various plots have been disrupted over the last decade and CADs have only become more sophisticated, less expensive, easier to operate, and more information has been made available online on how to augment them for different uses. Last year, FBI Director Wray warned of the threat posed by AVBIEDs.

> "We're investigating, even as we speak, several instances within the U.S. of attempts to weaponize — *to weaponize* — drones with homemade IEDs. That is the future that is here now."
>
> **FBI Director Christopher A. Wray, 17 November 2022**

The know-how and field experience in using AVBIEDs now reached a critical mass. The Islamic State (of whom 1,500 foreign terrorist fighters (FTF) have returned to Europe), Houthis, Hamas and Hezbollah, Mexican drug cartels, anti-regime forces in Myanmar, and soldiers fighting on both sides of the Ukraine war – some with ties to terror organizations and far-right groups – have all become adept at weaponizing and operating AVBIEDs. In addition, plenty of experienced drone hobbyists already possess the technical skills to weaponize a drone. Ultimately, it will only take one successful high-profile attack to create a snowball effect, inspiring other bad actors to leverage this consumer technology for disruption and destruction.

THE FUTURE WEAPON OF CHOICE

Weapons are purpose-driven tools. Malicious non-state actors will creatively use whatever means are at their disposal to efficiently maximize the impact of their actions while paying the lowest possible price. Between their availability and ease of use, the psychological and propaganda effects they produce, and the capabilities that drones give an individual, the AVBIED is the future weapon of choice for bad actors (see Figure 7). Today, there is a gulf between drone and counter drone technology and tactics, one that will soon be exposed.

COUNTERMEASURE GAP

CADs without any explosive ordinance already pose a major nuisance and security threat. Beyond the privacy risks associated with drone surveillance, malfunctions can lead drones to fall from the sky, posing a physical risk to those below. For these reasons, government regulators have restricted the airspace around airports, critical infrastructure, and sporting events and violating pilots can be charged with fines and criminal offences. But this measure has not prevented intrusion. In 2018, London Gatwick (LGW), the UK's second busiest airport, was shut down for 33 hours due to a drone flying around its runways, grounding 1,000 flights, costing airlines an estimated USD $64.5 million. In 2021, the National Football League reported 1,400 violations of game day airspaces. The NFL, MLB, NCAA,

THE EVOLUTION OF THE AVBIED THREAT

Figure 6

1994

JAPAN ✕ DIRECT

Aum Shinrikyo, a doomsday cultist, plans to use a remote-controlled (RC) helicopter to spray sarin or anthrax gas but the RC helicopter crashes during testing.

2003

UNITED KINGDOM ✕ INDIRECT

Moazzam Begg, an al-Qaida terrorist, plans to target the House of Commons with an anthrax-spraying drone but is apprehended.

2011

UNITED STATES ✕ DIRECT

Rezwan Ferdaus, an al-Qaida inspired terrorist, plans to acquire scale models of F-86 Sabre and F-14 Phantom jets (with GPS capability) and C-4 explosive for an AVBIED attack on the Pentagon and U.S. Capitol but is apprehended in a FBI sting operation.

2016

IRAQ & SYRIA ✓ INDIRECT

The Islamic State, Hezbollah, and other militant groups begin to use CADs as indirect AVBIEDs at scale.

BRAZIL ✕ DIRECT

The Islamic State encourages Telegram group followers to attach bombs to small CADs and attack the Rio Olympics. Police arrest 10 people over the plot.

2018

SYRIA ✓ DIRECT

Turkish-backed militants use a swarm of 13 homemade drones to attack Russian military bases.

VENEZUELA ✕ DIRECT

Two explosive-laden GPS–guided drones are used in failed assassination attempt on Venezuelan President Maduro.

2020

UNITED STATES ✕ DIRECT

A DJI Mavic 2 drone carrying nylon ropes and copper wire crashes into a Pennsylvania power substation, in an ostensible attempt to short circuit the transformers. The operator is still at large.

2021

YEMEN & MYANMAR ✓ INDIRECT

Rebel groups use DJI Mavic 2 quadcopters as indirect AVBIEDs to drop grenades with tail fins on government forces.

2022

UKRAINE ✓ INDIRECT

Footage of both sides of the conflict using various CADs as indirect AVBIEDs becomes ubiquitous.

Key

DIRECT — A single-use drone outfitted with explosive material designed to detonate on impact.

INDIRECT — A drone that delivers another weapon to its target.

✕ Failed attack/plot

✓ Successful attack/plot

THE FUTURE WEAPON OF CHOICE

Figure 7

EASE OF USE

- Piloted by a transmitter with a familiar layout (game console controller/toy remote controller) and relatively low learning curve.
- Some CADs have computer-aided piloting software, including self-correcting, autopilot, tracking (person or object) and obstacle avoidance making it easier for the drone to reach its target.
- Open-source software exists online (for those with computer skills) to remove drone safety features, including the GPS geofencing of restricted airspaces.

PSYCHOLOGICAL AFFECT

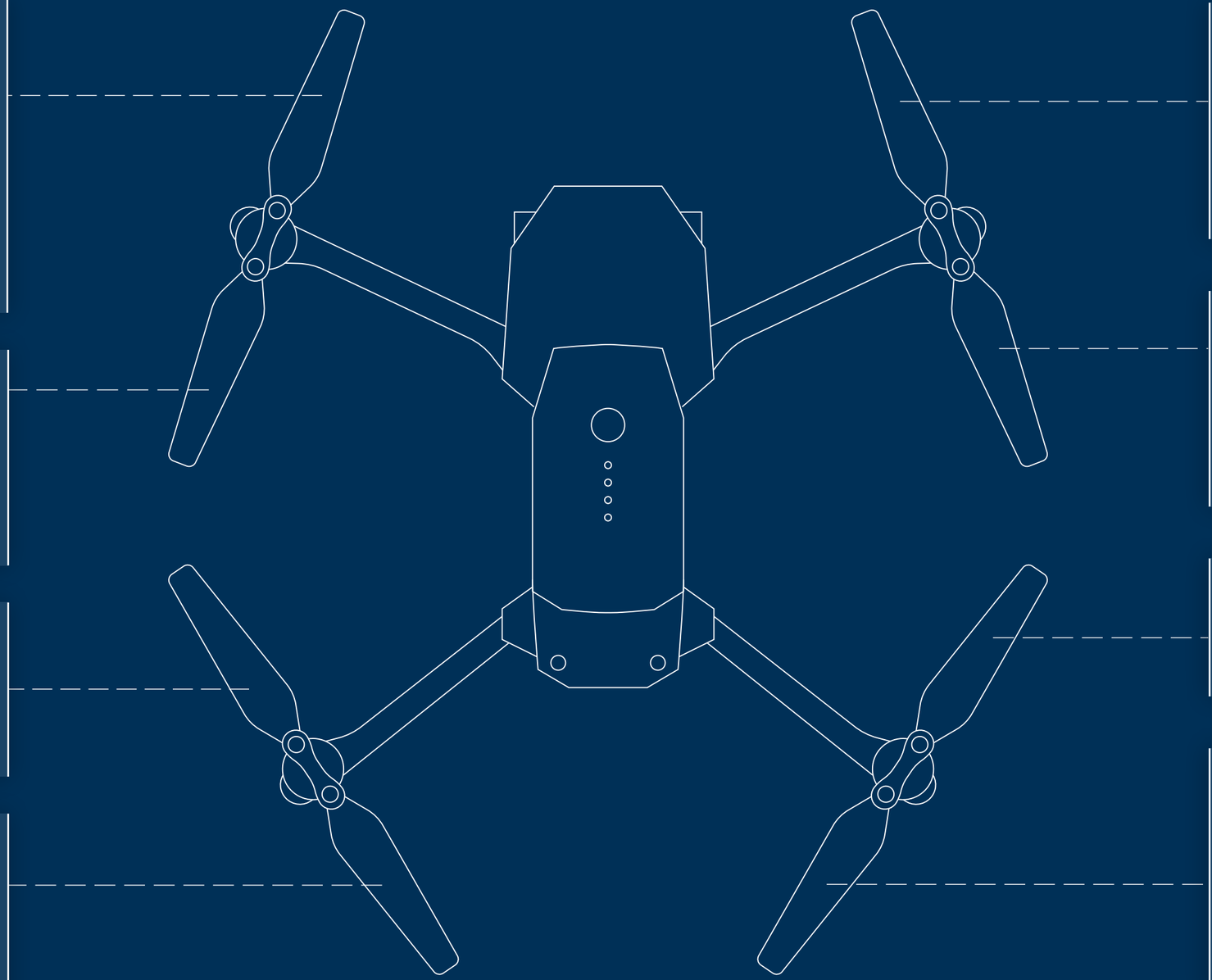
- A high-profile attack could traumatize a large population.
- The 1995 Oklahoma City Bombing changed the federal government's security standards; 9/11 irrevocably changed airport security. Even a failed attack on a symbolic site or an attack involving a fake aerosolized chemical or biological agent could change the security paradigm.

PROPAGANDA

- Footage of attacks can be collected and disseminated. The filming of successful attacks is a proven, powerful recruitment method for radical groups.
- Propaganda could even serve as the main goal of an attack.

STANDOFF & SURVIVABILITY

- Since AVBIEDs can transmit live video, they provide a beyond line-of-sight capability so actors can operate the drone from a safe distance (5 mi/8 km). Assailants can also bypass ground level security measures. This means that an actor can carry out a mission without risking their own life or even being caught.
- By removing the need for self-sacrifice, AVBIEDs expand the pool of would-be assailants to less zealous individuals.



LEVERAGE ASYMMETRY

- Asymmetric information: those planning know the target and timing an attack; those defending the attack must allocate resources to protect many locations at once.
- Cost asymmetry: the human resources and associated training, and systems needed to detect and neutralize AVBIEDs are several orders of magnitude more expensive than the costs associated with conducting an attack.

FORCE MULTIPLIER

- Greatly amplifies the extent of damage/destruction one person can cause and from a distance. Drones give non-state actors precision capabilities previously reserved for military use.
- Allow bad actors to bypass traditional land-based security measures giving access to secure areas.

COUNTERMEASURE GAP

- Existing counter-AVBIED capabilities are limited and techniques to use them have not been effectively tested and institutionalized.

AVAILABILITY

- Can be legally purchased and easily smuggled.
- Low cost: USD $1,000–$2,000 sticker price for a high quality, AVBIED-capable quadcopter; USD $5,000–$20,000 for a larger octocopter with more lift and range capabilities.
- Can be built DIY-style to reduce costs: online instructions are available for 3D printing drone bodies, though motors and computer parts will need to be purchased.

and NASCAR have all urged the government to expand current counter-drone capacities but bills in the U.S. Congress are stalled. Currently, only the Department of Homeland Security and Department of Justice are allowed to down drones in the United States. Even if this power is delegated to more federal agencies and state, local and tribal authorities, it is unclear if the existing technologies and accompanied practices will be sufficient to counter the threat of AVBIEDs.

The first issue with countering AVBIEDs is detection. Drones can be small, move quickly, and can fly upwards of 1,500 feet, making them difficult to see with the naked eye. They have low radar signatures and it is not possible to distinguish between an AVBIED and a benign CAD piloted by a hobbyist. Even after an AVBIED is correctly identified, neutralizing the threat is fraught with challenges. Current counter-unmanned ariel vehicle (C-UAS) systems include radio frequency jammers, net guns, and small arms fire.

Radio frequency jammers cut the connection between the drone and pilot and can be found in rifle-form or mounted on buildings or vehicles. The signal interruption normally causes a drone to land or go to a preprogrammed location that the pilot selects. But hand-held radio frequency jammers are limited by line of sight or may not jam the correct frequency that the drone uses. Mounted systems interfere with the transmission of nearby signals, not limited to Wi-Fi networks, car locks, and GPS-guided systems.

Net guns and small arms fire both require line of sight, are subject to inaccuracy and human error, and are less effective the higher the drone is. Even if these systems can down an AVBIED, they do not preclude its explosive material detonating on ground impact. High-energy microwave and laser systems are being developed but are not currently in use defending civilian sites.

In reality, Ukraine is a testing ground for both AVBIEDs and counter-AVBIEDs. It is too early to determine how effective directional jammers are, and comprehensive counter-AVBIEDs practices and strategies are being developed on the fly as the war rages on. It will be years until the lessons learned have been properly distilled and institutionalized and even longer until they find their way into local police forces. In other words, a countermeasure gap will continue for years to come.

SOFT TARGETS

Eventually, it is likely that the "highest value" targets – airports, outdoor sporting venues, key government buildings, and large organized gatherings – will be outfitted with nominal drone detection and countermeasure systems. Perhaps they will be adequate, perhaps they will not. But it will not be feasible to outfit all possible targets with protection. Fuel and water storage facilities, water filtration reservoirs, gas pipelines, power distribution lines and plants, cell phone towers, and food supply locations are but a few of the many sites that are unlikely to be protected and whose disruption could impact tens of thousands of people. Corporate offices and the private homes of business or political leaders will also be vulnerable, as government authorities are the only actors permitted by law to utilize counter-drone technologies.

THE FUTURE AVBIED

Drone technology is expanding rapidly and C-UAS systems are designed for the drones of today not of tomorrow. Heavy lift drones that can carry large explosives and can travel longer distances are already available and will continue to become more economical. Autonomous drones that cannot be jammed are already in military service and will soon hit the commercial market. The tactic of using drone swarms – coordinated attacks by swarms of many drones to overwhelm defenses – has already been emulated by terror groups. As access to artificial intelligence and automation improves, and the range and lift capacity of CADs increases, non-state actors will be able to pre-position AVBIEDs capable of delivering deadlier conventional (or even non-conventional) weapons and then command and coordinate them from anywhere on the planet as modern militaries do.

TAKEAWAYS

The universal use of commercially available drones in Ukraine foreshadows the successful use of weaponized drones against civilian targets by bad actors. AVBIEDs now pose an acute and ever-increasing threat to civilian infrastructure, corporate assets, and people, especially given that countermeasures are relatively untested, underutilized, and unavailable to private citizens and corporations. Just like the attacks on 9/11 forever changed aviation security, a high-profile attempted AVBIED attack could change the current security paradigm.

LITTLE BLUE MEN: CHINA'S GRAY ZONE FLEET

The Pacific is heating up. Recent Chinese incursions into North American airspace highlight the threats posed by China's increasing activity in the gray zone. Designed to damage an adversary's position without incurring an armed response, gray zone operations have become a key component of China's statecraft as it moves to reshape the Asia-Pacific regional order. The centrality of these operations to Beijing's Pacific strategy is illustrated by the expansion of China's Maritime Militia. Beijing uses this gray zone fleet to enforce China's territorial claims, menace Taiwan, and erode the weight of international law. The Militia blurs the lines between civilian and military, peace and war, and the beginnings and ends of sovereignty, setting the groundwork for instability.

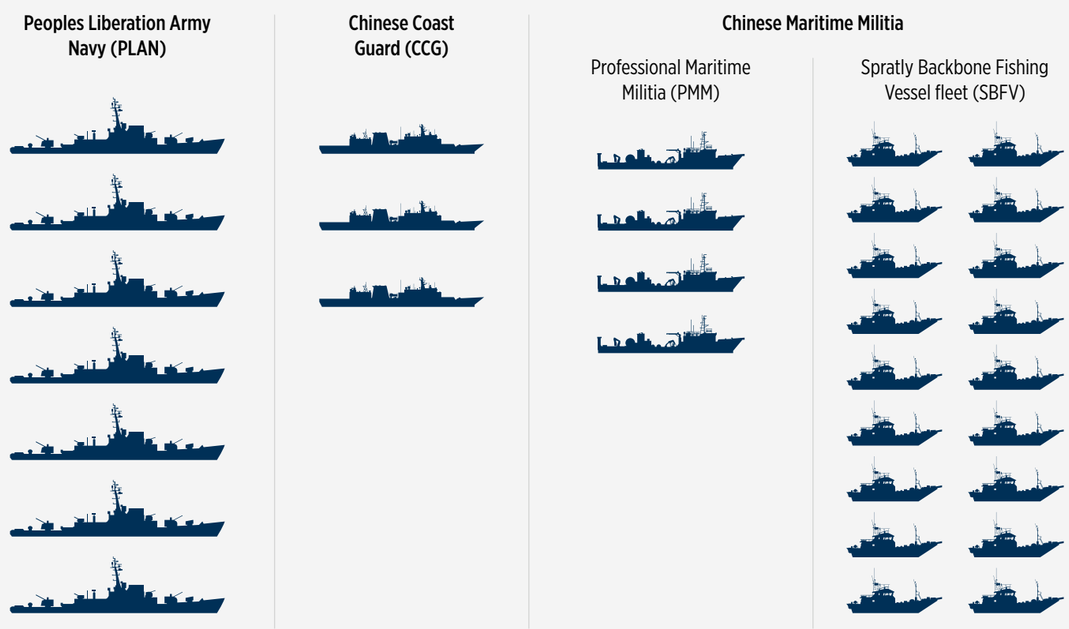
CHINA'S MARITIME MILITIA

In 2013, President Xi Jinping made China's transformation into a maritime power and the domination of its near-abroad into a national priority. In its pursuit of sovereignty over the South China Sea, Beijing faces the *de facto* naval superiority of the United States (U.S.) on one hand and the *de jure* legitimacy of rival claims on the other. With clear disadvantages in both war and peace, China has opted for the middle path.

Despite an international ruling in favor of the Filipino claim to the Spratly Islands, up to 100 Chinese commercial fishing vessels are active in the disputed territory

CHINA'S THIRD NAVY Figure 8

Each silhouette represents 50 vessels



Source: U.S. Department of Defense, Center for Strategic and International Studies

on any given day. These vessels – crewed by civilians and subsidized by the Chinese government – do relatively little fishing, but rather serve to manifest Chinese sovereignty through their presence. There are between 800 and 1,000 commercial ships in the Spratly Backbone Fishing Vessel (SBFV) fleet, which comprises the civil portion of the Maritime Militia (see Figure 8).

The Professional Maritime Militia (PMM) is numerically smaller than the SBFV with between 122 and 200 vessels. However, these ships are steel-hulled and generally measure over 55 meters (m), giving them the ability to ram other vessels. PMM crews are uniformed, armed, and trained professional militia members who are integrated into the People's Liberation Army Navy's (PLAN) command structure. PMM vessels are used to protect the SBFV from foreign navies and coast guards, and to harass foreign vessels in claimed Chinese waters.

Between the SBFV and the PMM China is able to negate the legal claims of its neighbors through force without employing the overtly military means that could justify an armed reaction by the U.S. However, having limited its opponents' access to peaceful mechanisms for conflict resolution, China has made escalation in the region all but inevitable.

FACTS ON THE WATER

China uses the Militia to establish "facts on the water" in support of Chinese claims on the territory inside the "9-Dash Line." In May of 2014, China installed an oil rig in waters claimed by both China and Vietnam. In response to the arrival of Vietnamese law enforcement, roughly 140 Chinese ships from the Militia, Coast Guard (CCG), and PLAN formed concentric rings around the platform (see Figure 9).

The ensuing standoff saw the use of high-pressure water cannons and ramming from both sides. Vietnam's own maritime militia, comprised largely of wooden fishing vessels, was unable to dislodge the militarized ships of China's professional Militia force. Ultimately, the Vietnamese would lose one ship to ramming. By the fall of 2015, China had created 3,200 acres of new land around its bases in the Spratly Islands, which included at least three 3,000-meter airstrips. By the end of 2017, China had largely completed the construction of harbors on Subi and Mischief reefs which continue to host large numbers of PLAN, CCG, and Militia ships. The presence of Chinese ships, oil facilities, and island bases effectively extends China's de facto Exclusive Economic Zone (EEZ) 1,000 nautical miles past its coastline with serious implications for international shipping.

> "The fleet's suitability for a spectrum of scenarios reduces the overall cost of escalation for China, increasing the probability of a conflagration at any level of crisis."

THREAT TO SHIPPING AND INTERNATIONAL LAW

In contravention of accepted maritime law, China treats its EEZ akin to its territorial waters, effectively nationalizing international territory. In 2009, roughly 60 nautical miles south of the limit of recognized Chinese territory, several Milita vessels harassed the USNS Impeccable as it conducted submarine monitoring operations. PMM vessels came within 15m of the U.S. ship, dropped debris in its path, forced an emergency stop, and along with PLAN and CCG ships, invoked maritime law in ordering the *Impeccable* out of the area. In another instance of illegal shipping interdiction, in June of 2019, a suspected Maritime Militia vessel rammed a Filipino fishing boat at anchor near the Spratlys. As the Filipino vessel sank, the suspected Militia ship went dark and fled the area. The Filipino crew was saved by a nearby Vietnamese vessel.

China's invocation of maritime law in the one case and use of plausible deniability in the second speak to two advantages of the gray zone fleet. First, China is able to erode the credibility of the international legal order by only acknowledging the law when it serves Beijing's purposes. Second, China's ability to effectively respond to different threat levels – both a U.S. naval vessel, and a Filipino fishing boat – with the same set of assets demonstrates the scalability of its gray zone forces.

THE CMM AND TAIWAN

The Militia allows China to operate aggressively at every level of escalation including full-scale war.

Island Grabbing: The Professional Militia whose crews are trained in small unit tactics could be used as "little blue men" to seize Taiwan's outlying islands while maintaining deniability similar to Russia's 2014 seizure of Crimea.

Blockade: Short of a full invasion, the Militia could form a critical component of a blockade of Taiwan alongside indefinite military exercises and live fire drills of the sort that followed Speaker Pelosi's visit in August of 2022. The Militia could reprise a scaled-up version of its role in the 2014 oil rig standoff, acting as an anti-access/area denial force. By disrupting the safe navigation of shipping into Taiwan, the Militia could help Beijing tactically disrupt the global semiconductor supply chain or apply significant food and energy pressure on Taipei in pursuit of political concessions.

Invasion: At the highest level of escalation, a potential invasion of Taiwan would see a heavy PLA reliance on the Militia for supply, sabotage, concealment, rescue, repair, and mining. PLAN sources indicate that Militia ships would be used as decoys, to launch false landings, absorb American anti-ship weaponry, and act as ostensive non-combatants to complicate U.S. decision-making. An analysis of PLA documents suggests that reliance on the Militia for these aspects of an invasion is not a provisional measure, but rather a key component of Chinese strategic planning.

The fleet's suitability for a spectrum of scenarios reduces the overall cost of escalation for China, increasing the probability of a conflagration at any level of crisis.

TAKEAWAYS

By investing in a dual-usage gray zone fleet, China has largely negated the *de facto* naval superiority of the U.S. and *de jure* territorial claims of rival claimants in the Asia-Pacific region. Since Beijing holds an advantage at levels of conflict short of war, China can be expected to escalate its provocations in the South China Sea and Taiwan Strait just until the point where an American military response seems inevitable. While this escalation is a destabilizing force on its own, it also raises the potential for a catastrophic miscalculation by either side, especially as Sino-American relations deteriorate.

OUTLOOK AND TAKEAWAYS

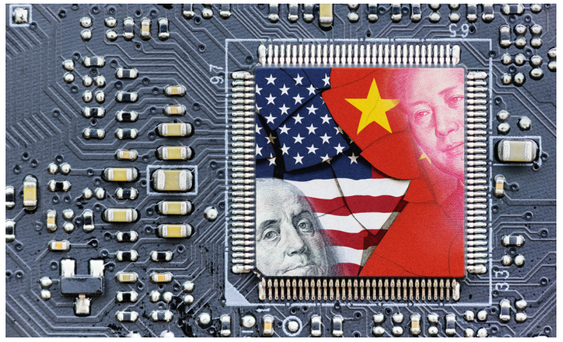
The "old way" of doing business with little to no thought of threats to personnel, infrastructure, communications, and supply chain is over. Today's evolving threat landscape presents an unprecedented challenge for organizations, especially multinationals. More than ever, geopolitics is shaping the international business environment. The second and third-order effects of the Russia-Ukraine War and the West's decoupling from China has only begun to expose the fragile state of globalization, necessitating organizations to proactively assess resilience and prioritize business continuity planning. Location matters. Not just the location of a business, its workforce, and assets, but the locations of an organization's partners, venders, and other aspects of its supply chain. Compliance, logistics, and strategic foresight are also becoming increasingly important as globalization meets Great Power conflict with corporations being caught in the crossfire.

NEW INTERNATIONAL ORDER

The peace dividend-yielding era of economic interdependence is nearing its end. The stability and prosperity brought forth by the globalization process are now being eroded by a return to an era of Great Power conflict. The fragility of the just-in-time supply chain and the inherent strategic vulnerability of a deindustrialized West have been irrevocably exposed. The low inflation age predicated on Russian-provided affordable energy in Europe and inexpensive goods produced in China that masked nominal wage stagnation in the West is over and a new Cold War is beginning. With tensions between Russia and the West and China and the West reaching a high watermark, Eurasia and East Asia are emerging as two regions to watch.

EURASIA

At the intersection of Russia, China, and Iran, Eurasia has already begun to destabilize as part of the fallout from the Ukraine War. The renewed hostilities between Armenia and Azerbaijan act as a preview for what is in store in the former-Soviet republics of Eurasia. With Russia – the main regional security guarantor – distracted in Ukraine, unrest, inter-ethnic tension, and competition over resources threaten to destabilize this resource-rich region. What is more, regional players – Iran, India, and Türkiye – as well as China and the U.S. are all eager to gain more influence and access to this increasingly important region. But an expanding Chinese commercial or military presence could destabilize host countries.



ASIA-PACIFIC

Washington is now weaponizing its leverage in the semiconductor space, where the U.S. and its close partners hold the keys to producing the tiny chips needed for advanced electronics. Having ramped up export controls on the Chinese semiconductor industry, the U.S. has both diminished Taiwan's utility to China and opened the door to Chinese retaliation in areas where it has leverage over the U.S., namely in raw materials, market access, and its use of gray zone warfare. In the near future, China's Maritime Militia could be used to disrupt international shipping in the key regional chokepoints or aid in any campaign to blockade or invade Taiwan. As the geopolitical competition with China heats up, the Asia-Pacific region will become more fraught with challenges for corporations.

TECHNOLOGY AND PROLIFERATION

Due to the democratization of technology, sophisticated weapons in both the cybersphere and the physical world are increasingly available to powerful non-state actors and rogue regimes alike. The weaponization of commercially available drones by non-state actors is one worrisome trend exemplifying the threats posed by increasing access to technology. With extensive use in Ukraine, drones will soon become a weapon of choice for bad actors of all stripes, especially given the fact that there are no proven defenses against them. On the state level, Iran and North Korea have made leaps in their respective nuclear programs. While it is too late to constrain Pyongyang, a preemptive attack on Tehran's nuclear program is becoming more plausible as Iran's support for Russia is creating a political environment more favorable for Israel (and possibly the U.S.) to act.

ABOUT GLOBAL GUARDIAN

Global Guardian is a leading duty of care firm that provides corporate, government, and family clients with real outcomes to a range of security and medical incidents and emergencies. Our comprehensive suite of innovative solutions—including real-time monitoring and location awareness technology, emergency response and evacuations, medical support and transportation, and global intelligence—are available at the push of a button and backed by our U.S.-based 24/7/365 Security Operations Centers and local response teams in over 130 countries.

GLOBAL INTELLIGENCE

Our team is standing by to support when global events have the potential to impact your organization, people, and operations. Global Guardian's intelligence analysts know the regional threats and local nuances throughout the world and can provide in-depth custom reports for clients and organizations in need of daily, weekly, or monthly real-time intelligence and analysis of events. To learn more about our intelligence products or start building your own custom report, email intelligence@globalguardian.com.

Global Guardian
8280 Greensboro Dr. Suite 750
McLean, VA 22102, United States

Global Guardian London
99 Bishopsgate
London EC2M 3XD, United Kingdom

Global Guardian Asset Security
2127 Ayrsley Town Blvd. Suite 201
Charlotte, NC 28273, United States

+1.703.566.9463
info@globalguardian.com
globalguardian.com