Aff Brief

Debate Hotline Resource Packet---AFF

1AC---Cartels

Cartels ADV

The US is launching strikes on cartels, decking US-Mexico relations.

Linthicum 10-28 [Kate Linthicum; Foreign Correspondent for the Los Angeles Times based in Mexico City, 10-28-25, "Mexican president condemns U.S. strikes that killed 14 alleged drug traffickers", Los Angeles Times, https://www.yahoo.com/news/articles/mexican-president-condemns-u-attack-141701976.html, DOA: 10-28-25] shaan

The Trump administration has **widened** its war against alleged drug traffickers, killing 14 people in attacks on four boats off Mexico's Pacific coast, a move condemned by Mexican President Claudia Sheinbaum.

The Pentagon said Tuesday that it carried out the strikes in international waters in the eastern Pacific Ocean on Monday. The U.S. and Sheinbaum initially said that one survivor had been rescued by Mexico's navy, though the navy later clarified that its search for the lone survivor was ongoing.

Sheinbaum **denounced the strikes** and ordered officials from her administration to discuss them with the U.S. ambassador to Mexico.

"We do not agree with these attacks, with how they are carried out," Sheinbaum said. "We want all international treaties to be complied with."

The Pentagon did not give exact coordinates of the attacks. Sheinbaum said only that they occurred in "international waters." In a post on X, Mexico's navy said that at the behest of the U.S. Coast Guard it was conducting a search-and-rescue operation 400 miles south of the Pacific resort city of Acapulco.

The Pentagon declined to share the nationalities of the victims, any evidence that they were in fact trafficking drugs and whether they were suspected of allegiance to a particular cartel.

The latest strikes mark a **new escalation** of the U.S. military campaign against alleged Latin American drug runners, which White House officials have branded "narco terrorists." In recent months, President Trump has formally designated several **drug cartels** as terrorist groups and the military has ordered thousands of troops, war ships and fighter jets to the Caribbean sea in an effort to combat them.

At least 57 alleged traffickers have been killed in 13 strikes in the Caribbean and the Pacific, mostly off the coasts of Venezuela and Colombia. Most experts agree that the strikes violate U.S. and international law because the military is not supposed to target civilians — even alleged criminals — who are not at war with the United States.

Trump has said that he does not plan to ask Congress for a "declaration of war," and that **he alone** has the authority to declare drug traffickers as enemy combatants.

The strikes have provoked **outcry throughout Latin America**, with Venezuela's authoritarian leader, Nicolás Maduro, insisting that they are political in nature and designed to push him from power. After Colombian President Gustavo Petro criticized the U.S. for "murdering" civilians in strikes off the coast of his country, the U.S. Treasury Department responded by sanctioning him and several members of his family, and Trump threatened to impose punishing tariffs on Colombian imports.

Before this week, Sheinbaum had avoided a **full-throated condemnation** of the Trump administration's high-seas attacks.

U.S. officials have warned for months that they may carry out strikes on drug trafficking targets in Mexico, which is the principal smuggling corridor for America-bound drugs, including cocaine and synthetic drugs such as methamphetamine and fentanyl.

The Trump administration has ramped up CIA surveillance drone flights over Mexico, formally designated drug cartels as "foreign terrorist" groups and floated the possibility of deploying troops there to fight organized crime.

Mexico is "essentially run by the cartels," Trump has said, insisting that the United States should "wage war" against them.

Sheinbaum has repeatedly said that she opposes unilateral U.S. actions in Mexico and would treat a military incursion as an **act of war** — a nationalist position that has played well with her base.

That causes domestic instability and escalation of conflicts---only closer cooperation and intel-sharing with Mexico solves.

Livermore 25 [Doug Livermore; National vice president for the Special Operations Association of America, 1-14-2025, "US intervention against Mexican cartels carries major risks. Here's how to mitigate them.," Atlantic Council, https://www.atlanticcouncil.org/blogs/new-atlanticist/us-intervention-against-mexican-cartels-carries-major-risks-heres-how-to-mitigate-them/, DOA: 10-28-2025] shaan

Is direct military intervention against Mexican drug cartels the answer to ending the US opioid crisis and improving security along the border? Several members of the incoming Trump administration have suggested deploying US special operations forces to combat cartels. The proposals are similar to how the United States has previously engaged in counterterrorism and counterinsurgency abroad, reflecting just how much the drug trade—especially fentanyl originating from China—has negatively impacted US communities.

But such **unilateral military action** would come with **risks**, as the cartels have a **significant capability to retaliate**. In addition, even considering military action would first require strengthening complementary efforts with the Mexican government and domestically among local and federal government agencies in the United States.

Mexican cartels are not merely criminal organizations; they operate as paramilitary entities with **deep financial resources**, **global supply chains**, and **sophisticated logistical networks** that extend into the United States. It is unlikely that such groups would passively absorb US attacks. Instead, as history shows, cartels are highly likely to retaliate both preemptively and reactively. They possess a substantial capacity for terrorism that, when coupled with their established presence within the United States, could **escalate conflict** far beyond what proponents of a purely military solution may anticipate.

Given their extensive experiences and expertise in combating elusive terrorist networks, oftentimes operating quietly in the shadows while supporting partners on the ground, US special operators are ideally suited for this fight. However, US special operators and their families would likely find themselves in the cartels' crosshairs. But there are ways that the United States should prepare for such retaliation before Washington even considers such action.

A proven capacity for retaliation

Mexican cartels have demonstrated an uncanny ability to adapt and retaliate against perceived threats, as demonstrated throughout Mexico's history.

Soon after Felipe Calderón became president of Mexico in 2006, he declared a "war on drugs," deploying military forces against cartels. The result was a **sharp escalation** in violence. The cartels retaliated by targeting law enforcement, military personnel, and government officials. Entire police forces **resigned in fear**, and public officials were assassinated in broad daylight. Beyond physical violence, cartels also employed psychological tactics, using brutal killings and public displays of bodies to instill terror among the population.

On October 17, 2019, Mexican forces arrested Ovidio Guzmán López, the son of drug lord and former cartel leader Joaquín "El Chapo" Guzmán. The Sinaloa Cartel swiftly unleashed widespread violence. Using armored vehicles, machine guns, rockets, and other heavy weapons, approximately seven hundred cartel "sicarios" conducted widespread attacks against civilian, government, and military targets across Culiacán. The cartel's campaign of terror overwhelmed Mexican authorities in what has become known as the "Battle of Culiacán" and "Black Thursday." This incident underscored the cartels' operational sophistication, which ranges from coordinating large-scale attacks to leveraging public fear. And amid all the violence, the government released Guzmán.

Throughout Mexico's recent history, cartels have routinely retaliated against perceived threats to their operations, including media organizations and civilian populations. Of the reporters who have been slain, some had written negative reports about the drug cartels themselves, while others have exposed corruption among those politicians that the cartels pay off. By controlling narratives and instilling fear, they secure

compliance and deter resistance. In some years, Mexico has proven itself to be even more deadly for reporters than active warzones such as Syria and Ukraine.

Given these examples, it is not difficult to imagine how cartels might respond if US forces launched cross-border operations. The difference, however, is that the retaliation could happen within US borders.

Hitting home

The US homeland is not immune to the consequences of engaging in direct military action against Mexican cartels, and such a campaign would not see the cartels simply ceding the initiative and sitting on their side of the border waiting to be attacked. The very networks that facilitate drug trafficking, spanning from cities (such as Los Angeles and Chicago) to rural communities, provide cartels with the infrastructure for potential **retaliatory strikes**. Cartels have a history of assassinating government officials in Mexico, and they would likely adopt terrorist tactics in the United States against political figures, law-enforcement leaders, and even military personnel. Extensive cartel connections to **Chinese underground banking** and US-based gangs could readily facilitate such **actions** against targets inside the United States.

Beyond physical attacks, cartels could engage in cyber operations, employing such capabilities to gather information on potential targets as part of criminal dealings. Their financial power also enables them to influence local politics and law enforcement through intimidation and corruption. Cartel cyber activity could bear significant effects for the target of such operations; and if the target (for example, a government department or agency) suspends its normal operations to repair its security walls, those effects could expand across communities.

Increasingly, Mexican drug cartels have turned to the “cybercrime as a service” economy, infiltrating government and commercial institutions to advance their criminal interests. By potentially coordinating cyber activities with campaigns of terror in cartel-influenced US neighborhoods, these groups could sow panic and destabilize communities, driving Americans to call for a cessation of operations against the cartels in Mexico.

What must come first

Any US military campaign to combat the cartels would **only succeed** if accompanied by a robust partnership with the new Mexican administration, led by President Claudia Sheinbaum (who has expressed a desire to fight organized crime more aggressively). Joint task forces, **enhanced intelligence sharing**, and specialized training programs can bolster Mexico’s counter-narcotics capabilities. Equally important is addressing systemic corruption within Mexico, which has long hindered efforts to dismantle cartel operations. By empowering its partners, the United States can achieve a **greater impact** without exacerbating the violence that unilateral actions alone often provoke. When and where no other options exist, the United States should launch appropriate unilateral operations against high-value cartel targets at the invitation of the Mexican government and in support of counter-narcotics objectives shared by the United States and Mexico.

The AFF solves---it dismantles cartels from within and increases data collection. Cartels rely on current networks which means they can’t switch communications.

Walker 20 [Summer Walker; Head of Security and Rights Initiatives for the Global Initiative, 2020, "Transformative Technologies: How digital is changing the landscape of organized crime," https://globalinitiative.net/analysis/cyber-tech-organized-crime/, DOA: 10-29-2025] shaan

How the growth of digital technologies has **changed market dynamics**

While the emergence of online markets on both the surface and the dark web, together with the growing availability of a range of digital and information communication technologies, has not transformed the underlying infrastructure of the international drug-trafficking trade, it has catalyzed a number of shifts in market dynamics.

Many drug-trafficking groups exploit technology and **apps to communicate** – El Mencho, of **the Sinaloa cartel**, communicates with his senior traffickers by **WhatsApp** group.32 With **end-to-end encryption**, and easily installed, this is a simple and direct way in which to command **horizontally structured organizations**. WhatsApp is used by dealers and users in many countries as a means through which the various risks related to drug transactions (including arrest and hijacking) are diminished.

Trafficking networks are increasingly likely to rely on **online financial transactions**, including with the use of payment apps on smartphones, like EcoCash, which is common in Zimbabwe.33 This allows consumers and dealers to avoid carrying cash, reducing the risk of cash being used as evidence in the event of arrest, and of being hijacked.

Turning to darknet markets, these have the greatest effect on the final links in the supply chain, and on consumer markets.

Online markets have transformed the drug market from a network economy, in which **limited advertising** and **clandestine operations** mean transactions typically occur through **existing networks** and thereby **favour incumbents**, to a conventional market where dealers compete on price, quality and service. This has eroded the incumbent advantage and lowered barriers to entry.34

Social-media platforms are being used to recruit new sellers. Research in the UK found that social media has reportedly been used to advertise the luxurious lifestyles of drug dealers and to groom child dealers as a way of cutting out the middleman, thereby penetrating local markets directly.35 In two separate trafficking arrests in the US, the person arrested claimed to have responded to an advertisement on Facebook for 'people looking for work' or 'an opportunity to make money', and ended up trafficking illicit drugs for cartels in Mexico.36 Social media is thus able to create new opportunities for transactional relationships between criminal groups and new ad-hoc employees.

Recreational users buy illicit drugs on darknet markets for a combination of reasons related to safety, quality and ease of purchase. The online market allows for anonymity in both sales and purchases, reduces **direct contact** between players in the market (thus possibly reducing risks associated with open-air drug markets), and in some cases has allowed for enhanced accountability in rating a seller's product or products – an interesting potential benefit from a public-health perspective. However, the ease with which vendors are able to post fake reviews and information online is poorly understood by users, and this can easily increase a user's chance of being misinformed.37 Purchases tend to be based on 'price, details of product, vendor reputation, feedback from other buyers, and available "trip reports" (descriptions of personal experiences with the effects of specific substances)'.38 Some listings are even described as 'fair trade' or 'conflict free'. The prevalence of illicit-drug supply on social-media platforms, which are heavily used by those between the ages of 16 and 24, could result in growing markets among younger drug users.39 Built-in design features on these platforms, including 'suggested friend' functions and hashtags to expand reach, can be used by dealers to expand their customer base.

The advantages for sellers on darknet markets are that they can avoid detection and minimize risks, such as 'arrest and violence, and threat to profits and reputation'.40 As noted above, this may have lowered barriers to entry for small-scale players in the drug-trafficking markets; a hypothesis supported by the limited use of the darknet by larger criminal groups.

According to RAND, both buyers and vendors of illicit drugs on the darknet share a common profile. This has been identified as someone young, male, hailing from English-speaking or West European countries, well-educated, entrepreneurial and with strong IT skills.41 This is, to a significant extent, shaped by the prevalence of darknet markets for final-leg distribution in consumer countries. Some research suggests that online vendors are either established dealers with access to the product, or newcomers who are expanding their base beyond selling to friends.42 There is concern that a younger and more tech-savvy consumer base could access illicit substances more easily, but evidence has not yet revealed this to be a trend.

Buyers purchasing drugs on the darknet typically use bitcoin or other types of **cryptocurrency to pay** for the product. In some cases, including in the case of the original Silk Road, payments are held in escrow by darknet administrators until the product is received. Then, the purchased substance is mailed through either private or public mail systems. Products can be delivered to a number of **anonymous locations**, including anonymous post-office boxes, automated booths or 'packstations'.

By collapsing **geographical distances**, online criminal markets empower smaller dealers to supply local markets while trading on the **global drug-trafficking market**. They also rely on small-parcel post, which has a significantly low surveillance rate, thereby further reducing the risk of engagement.43

Reduced operating costs means drug prices are predicted to decrease.44 Online dealers require fewer employees and benefit from lower overheads, as is also the case with licit online businesses.

Legal and enforcement challenges

When trying to tackle operations conducted on the surface web, law-enforcement entities often rely on the **cooperation of private-sector** e-commerce platforms and social-networking sites. However, such cooperation has always been **ad hoc** or at the discretion of the respective platform.

When platforms have cooperated in attempting to mitigate their use by drug-trafficking operators, the speed at which sellers adapt to these changes **lessens the impact**. For example, in 2017, Facebook disabled certain key search terms – for example, 'OxyContin', 'Xanax' and 'fentanyl' – on its search engine and replaced some search results with adverts for substance-abuse treatment. Sellers adapted quickly by putting the name of their product in their Facebook profile name, thereby enabling searches to function as before.45

The use of dynamic coded language and emojis by dealers operating online, including on social media, presents a further challenge to both law enforcement and social-networking platforms in identifying accounts supplying illicit drugs.46

Large-scale law-enforcement operations have successfully shut down a number of marketplaces on the dark web, but this has led to the fragmentation of the darknet market. This is evident in the growth of the number of 'vendor shops (shops run by a single vendor), and secondary markets, i.e. nonEnglish-language markets catering to a particular nationality or language group'.47

There is significant concern among law-enforcement entities that sellers distributing illicit drugs on the darknet will react to such shutdowns by moving away from large marketplaces, and instead offer products to consumers directly over **encrypted messaging** apps, such as Telegram. The already widespread use of encrypted networking platforms, including WhatsApp and Snapchat, by the illicit drugs market poses a barrier to the **gathering of data** by law enforcement, particularly as platform owners have typically **refused to share** user data in the context of police investigations. These messaging apps are therefore extremely difficult for police to monitor.

Chaos causes proliferation and emboldens adversaries.

Robert **Haddick 10**, Former advisor of the State Department, "This Week at War: If Mexico Is at War, Does America Have to Win It?," Foreign Policy, 9/10/10, https://foreignpolicy.com/2010/09/10/this-week-at-war-if-mexico-is-at-war-does-america-have-to-win-it/, tristan

Most significantly, a **strengthening** Mexican insurgency would very likely affect America's role in the rest of the world. An **increasingly chaotic** American side of the border, marked by **bloody** cartel wars, corrupted government and media, and a **breakdown** in **security**, would likely cause many in the United States to **question** the **importance** of military and foreign policy ventures elsewhere in the world.

Should the southern border become a U.S. president's primary national security concern, **nervous allies** and **opportunistic adversaries** elsewhere in the world would no doubt **adjust** to a **distracted** and inward-looking America, with potentially disruptive **arms races** the result. Secretary Clinton has looked south and now sees an insurgency. Let's hope that the United States can apply what it has recently learned about insurgencies to stop this one from getting out of control.

Extinction.

Stephan **Cimbala 23**, PhD, Professor at Penn State University, "Politics Between Nations: Power, Peace, and Diplomacy?," Springer, 6/xx/23, https://tinyurl.com/eur8r2cu, recut auraine

Unstable **command and control** over **nuc**lear force**s** could be **joined at the hip** to **nationalist** or **religious hostility** in Asia. During the Cold War, the Americans and Soviets competed on the basis of political ideology: communism versus capitalism. Both of these ideologies were rooted in Western philosophy and history and neither, with the exception of lunatic fringes on both sides, anticipated an inevitable final day of judgment between the two systems. Despite significant differences in military strategic doctrine, the USA and the Soviet Union established an ongoing process of nuclear arms control that helped to stabilize their political relationship and to avoid conflicts based on misinformation and mistaken assumptions about one another's intentions. In a sense, more than four decades of "nuclear learning" occurred as between the two nuclear superpowers that lasted to the very end of the Cold War and even beyond the demise of the USSR.7

In Asia, the next decade or two may witness the combination of **absolute weapons** in the hands of leaders with apocalyptic motivations or regionally **hegemonic** objectives. To be clear: it is not asserted here that the leaders of nuclear powers in Asia will be less "rational" than their European counterparts. Rationality is a loaded, and a subjective, term. In politics, it implies a logical or logically intended connection between political ends and means.8 **Leaders in Asia** will have **political objectives** that

differ from those of the Cold War Americans and Soviets: not illogical in their own terms, but less **road tested** against **accidental**, inadvertent, or **deliberate escalation** to nuclear war under the stress of political crisis and **ambiguous intelligence**.267

Military strategy is the realm of logical paradox and oxymoronic truths. Strategies and policies intended as defensive can, in this paradoxical world, appear provocative and offensive to other states. For example, leaders in Asia might misconstrue or apply mistakenly the strategy of **preemption**. It is not an offensive strategy but a defensive one. Preemption is motivated by the expectation that the opponent has already launched an attack or is about to. It is dangerous on account of its "defensiveness": leaders **misperceive** that they are already **under attack** based on **deficient** and **misleading indicators** of warning, or on **mistaken** assumptions about enemy intentions and capabilities.9

Another possible path to war based on the twenty-first century military realities is the deliberate use, or threatened use, of weapons of mass destruction, including nuclear weapons. We noted already that this use might occur as part of "anti-access" or "area denial" strategies in Asia. **Hostile powers** could employ the threat of **nuclear first use** against American **allies** or forward deploying the US forces in order to deter American intervention in the region, against their interests.

This is an obvious stratagem for China to use in case it decides to forcibly disarm Taiwan or otherwise create a military fait accompli in the Western Pacific contrary to the US interests.10 China would not need to use nuclear or other weapons of mass destruction in order to accomplish a number of its possible objectives in the region, absent the US military intervention. The challenge for China would be to deter or defeat US military intervention in favor of Taiwan or another threatened interest. More accurate ballistic missiles of various ranges, improved air defenses and C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) and expertise in cyberwar could augment Chinese access denial capabilities—with or without nuclear weapons.11 In addition, the **combination** of **nuclear** and **cyber capabilities** in a USA–China confrontation could create a **scenario of escalation** from conventional war into a **nuclear** crisis. As Andrew Futter has noted:

This is a particular concern given the fact that China is thought to share some parts of its C2 system for both nuclear and conventional forces. This risk is, in turn, likely to have implications for China's 'No First Use' nuclear posture, particularly when cyber is combined with US ballistic missile defence plans and conventional global strike capabilities.12

Nor is this all—some Chinese policy and strategy discussions suggest a potential for **seamless transition** from conventional to **nuclear war**, once an enemy has attacked China's vital interests. China's expectation is that the most important regional wars of the future will be conventional conflicts under the shadow of nuclear deterrence. Therefore China may adhere to a notion of "double deterrence" based on the combined or sequential use of conventional and nuclear missile brigades, with nuclear weapons as "a backstop to support conventional operations." 13

North Korea, whose small nuclear arsenal might also play an "access denial" role, is the best current example of an otherwise strategically insignificant state whose nukes have placed it in a pivotal position for regional stability. Without an agreement to verifiably dismantle its declared nuclear weapons capability, North Korea threatens serial production of nuclear weapons for access denial to the Americans, for political intimidation of South Korea and Japan, and for possible sale to third parties, including terrorists. The USA and South Korea could defeat North Korea in a war if it came to that, but such a war on any scale would be devastating for South Korean civilians. Therefore, Seoul prefers détente and an open door for eventual unification of the two Koreas, as opposed to coercive diplomatic or military pressure against Pyongyang.

It may turn out that North Korea eventually abandons its apparent commitment to membership in the ranks of nuclear powers, although the nuclear saber rattling of Supreme Leader Kim Jong-un is disconcerting in this respect. It is also too early to tell whether the P-5 plus one (the USA, Britain, France, Russia, China, and Germany) agreement with Iran in 2015 to freeze its nuclear ambitions short of weaponization will have transitory or enduring effects. If these two cases **slip the leash** of **nonproliferation**, others are almost **certain to follow**, and the geostrategic logic of political rivalry in **Asia** and in the **Middle East** will be tightly bound up with a **high probability** of **WMD**, including nuclear, **use**. The USA and **allied diplomacy** with regard to actual and potential **nuclear states** in Asia will have to **combine carrots** with **sticks** in order to induce, or dissuade, a repeat performance of July and August, 1914 but on a grander scale.14 A **worst-case** scenario is **not** inevitable; there is no deterministic relationship between more weapons and a greater likelihood of bad decisions.15

The next section provides some operational definitions for variables and models one possible, although not necessarily inevitable, Asian nuclear arms race if proliferation is not contained.

Proliferation in Asia

The Cast of Characters

In this section, a model of eight potential nuclear states in Asia, circa. 2025–2030, is posited for heuristic purposes. It is not a point prediction, but a device for generating hypotheses and insights. The states in question include the acknowledged and de facto nuclear weapons states with strong military presence in Asia: the USA, Russia, China, India, Pakistan, and North Korea. In addition, nuclear weapons have also spread to the following nuclear-threatened or nuclear-aspiring states in Asia: Japan and South Korea. These assumptions might be falsified in the future: more, or fewer, states in Asia might acquire nuclear weapons in the next fifteen years or so. However, for ascertaining the effects of interactions among Asian powers with respect to nuclear deterrence, these selections appear to be substantively appropriate.

<<FIGURE OMITTED>>

The USA behaves strategically in Asia, to be sure, and deploys significant forces there. And some might reasonably argue that globalization will drive more the US security challenges into Asia, now that post-Cold War Europe is presumably debellicized. But the USA is still a unique actor, capable of marshaling conventional as well as nuclear forces with global reach and precision strike. This uniqueness in capability and in an expansive definition of its international security interests puts the USA in a singular category: but not necessarily, as some have argued, as a global hegemon.16 Truly international hegemony is beyond the scope of any single power today, because power includes both “hard” economic and military power and “soft” power of cultural values, diplomacy, and moral suasion.17

Figure 1, below, is a matrix of interactions among eight existing and possible future nuclear states in Asia.

In theory, each of the eight states above might have a deterrence problem or potential problem with any one, or more than one, of the others. Deterrent situations could be **dyadic**, involving two powers, or more **complicated**. The size and shape of opposed political coalitions would determine the military requirements for each state. Suppose, for example, that **Japan** and **So**uth **Ko**rea allied against **North Korea**. North Korea might then **receive support** from China, and perhaps Pakistan. India would probably **balance** against China and Pakistan. Russia would have conflicting priorities: political and economic commitments to India and China; concern about instability on the Korean peninsula; suspicions about PRC intentions but preferring détente between Moscow and Beijing; and opposed to Japan’s going nuclear.

<<FIGURE OMITTED>>

Each cell in the matrix of possible deterrent threats or actions might be filled in by P (generally positive expectations about the threat of an immediate deterrence situation, although all states exist in a general deterrence condition requiring at least passive vigilance); or N (generally negative expectations about the threat of an immediate deterrence situation); or A (ambivalent expectations). The resulting matrix might appear as it does in Fig. 2, below.

Expert analysts could disagree about the values assigned to cells in the matrix, and today’s values might not be the same as tomorrow’s. The matrix is illustrative, not definitive. The three-option ordinal scale offered here could be refined into an interval scale of trust or suspicion with regard to the expectation of involvement in an immediate deterrence situation. For example, each cell might be scored from one to ten with one representing the most positive affect (least fearful of a challenge from the designated state) and ten representing the most negative threat assessment (most pessimistic about a challenge from the state in question). A panel of expert judges could assign various values for each cell in the matrix and over long periods of time, providing a longitudinal analysis based on pooled judgments.

Judgments like those discussed above are not merely exercises for analysts. Political leaders and military planners make these kinds of judgments every day. Threat assessments, even against nominal allies, are accompanied by espionage against allies, adversaries, and nonaligned states. Note how alliances, both soft and hard, complicate assessments as simplified in the preceding matrices. If, for example, many of the “ambivalent” states (positive or negative) with respect to various partners were to shift suddenly into the positive (P) or negative (N) column, dramatic adjustments in the definition of adversaries and in the requirements for deterrence would result. Something like this happened in the years immediately preceding World War I, when alliances that had previously been inchoate and flexible began to harden and reify into antagonistic blocs. As a result, the flexibility of alignment necessary for stability in a multipolar system disappeared into the rigidity of dichotomous thinking about friends and enemies.

Threat assessments pertinent to nuclear deterrence assume reliable intelligence about the actual intentions and capabilities of adversaries. **Intell**igence about states’ intentions is notorio**usly suspect**, on the evidence of history. Intentions of policy makers are often deliberately veiled, especially if those intentions include plans for preemptive attack. In theory, military capabilities should be more “objective” to enumerate and to assess than are the intentions of states. But capabilities can also lend themselves to misestimation. **Many states** have **gone to war** based on **faulty** net assessments that **underestimated** enemy capabilities and overestimated their own. The capabilities of military forces are bound up with the skills of the commanders who are using them and the political leaders to whom those commanders are accountable. As to the latter: Napoleon and Hitler, despite the excellence of their militaries, managed to drive their armed forces into the ground and their states into political defeat by insisting upon objectives and war plans that were beyond the reach of their military capabilities.

In the case of nuclear forces, capabilities are measured not only by their destructiveness in war but also by their credibility in deterrence. Since proving a negative is difficult, the absence of war in a given case may, or may not, suffice to prove that deterrence "worked." Nevertheless, most political leaders and military planners would prefer to achieve their objectives while avoiding an outbreak of nuclear war: unless those leaders and planners are highly risk acceptant or motivated by absolutist goals not amenable to compromise. Since nuclear deterrence is preferable for most to nuclear war, capabilities for nuclear deterrence matter more than capabilities for nuclear war fighting. However, the matter is complicated by the fact that a convincing nuclear deterrent must be capable of performing its retaliatory missions when called upon to do so.

Measuring the relationship between nuclear capabilities and their contribution to deterrence involves several steps, carried out in the next section. Hypothetical nuclear forces are posited for these eight possible nuclear-armed states in 2025–2030 and are subjected to force exchange modeling in order to see how well they would be expected to perform under various conditions. From these findings, some hypotheses and generalizations about stability in a future multipolar nuclear Asia can be inferred.

Forces and Outcomes

For purposes of analysis, a notional force mix of land-based missiles, sea-based missiles, and bomber delivered weapons is assigned to each of the eight states. The US and Russian forces are assumed as constrained by New START limits on deployed warheads and intercontinental launchers and New START counting rules (at least through 2026).18 Over-specification and excessive detail for each arsenal would be mistaken, for several reasons. First, the precise weapons systems deployed by each power in the years ahead will be determined by their future threat perceptions, economic and technological capabilities, and political ideologies and affinities. In addition, for states with intra-regional rivalries, land-based missiles and bombers with short or medium ranges suffice to deliver "strategic" blows as well as the longer range intermediate and intercontinental launchers. Third, not every state may prefer a "triad" of land and sea-based missiles and bombers, but we have assigned each state in the analysis a "triad" of sorts in order to "level the playing field" of force survivability. For these and other reasons, our notional forces are broad-gauged composites and not point predictions about detailed capabilities.

Table 1, below, summarizes the sizes of the operationally deployed strategic (i.e., capable of strategic or decisive effect) weapons for each state. The sizes of their total forces and their mixes of launchers vary with our estimates of their future capabilities and strategic settings. For example, states with large national territory (Russia, China) can deploy land-based missiles more survivably than states with less territory (Japan). And states with advanced technology can deploy with more confidence a fleet of ballistic missile submarines than states with a less developed research and development capability.

In addition, Table 1 also calculates the numbers of surviving and second strike retaliating warheads for each state. Each of the notional prewar forces is subjected to counterforce first strikes from state or states "X" (unknown). The surviving and retaliating forces left to each state after absorbing a first strike are calculated using standard methodology for estimating how many land-based missiles (ICBMs or missiles of shorter range), submarine-launched missiles (SLBMs), or bomber delivered weapons remain. Although we do not know the exact identity of future attackers against any one or more of these states, analysts can estimate with reasonable confidence (based on historical studies and knowledge of weapons and commandcontrol system performances) the probable percentages of surviving weapons systems in each case. The methodology used here is extrapolated from road tested force exchange models used in other studies.19

As might be expected, the larger forces have more total survivable and retaliating warheads, compared to the smaller prewar forces. However, not all weapons systems survive equally. Much depends on each state's mix of launch platforms and, as well, the conditions under which retaliatory launch takes place. Four possible conditions are examined in Table 1: (1) forces are on generated alert and launched on warning (so-called maximum retaliation); (2) forces are on generated alert, but are launched only after riding out an attack (intermediate retaliation); (3) forces are on day to day or normal peacetime alert, but are launched on warning of attack (also intermediate retaliation); (4) forces are on day to day alert and ride out the attack (minimum retaliation).

<<TABLE OMITTED>>

The summaries in Table 1 provide important indicators about static stability, but are not necessarily informative with respect to dynamic nuclear stability. To estimate the latter, we need two measures of dynamic stability as between the performances of nuclear retaliatory forces. The first measure is generation stability: the ratio of the number of weapons surviving and retaliating after riding out the attack, compared to the decision for launch on tactical warning of attack, under each of two conditions: (1) forces are on day to day alert; or, (2), forces are on generated alert. The difference between the two conditions is expressed as a percentage: the higher the percentage, the more stable the situation. The second measure of dynamic stability is "prompt launch stability," or the numbers of weapons surviving and retaliating on day to day alert, compared to generated alert, under each of two conditions: (1) forces ride out the attack and then retaliate; or, (2), forces are launched on tactical warning of attack.

The measures of dynamic stability enable us to go beyond the mere calculation of second strike survivability and to ask about the relational expectations of potential adversaries. In particular, we can see the relationship between alternative force sizes and force structures, in addition to the options available to decision makers with respect to their dependency on prompt compared to delayed launch, or on generated alert compared to day to day alert.

Estimation of dynamic stability will, of course, require more fine-grained analysis of dyadic relationships as between potential adversaries. For example, in 2017 the US relationship with North Korea deteriorated in the wake of repeated North Korean missile and nuclear tests and predictably negative USA and United Nations responses. Was nuclear deterrence stability as between the USA (and its Asian allies) and North Korea at risk of inevitable failure, given a continuation of North Korean brinkmanship and military adventurism? Part of the problem was the lack of intelligence about North Korean decision-making. North Korean leader Kim Jongun might understand the US logic of nuclear deterrence rationality very incompletely, if at all. On the other hand, Kim Jong-un might understand American deterrence rationality but not accept it: his version of brinkmanship was self-taught, without the nuclear learning that the USA, the Soviet Union, and China had gone through during the Cold War.

We might use the simple matrix below to illustrate some of the challenges facing the US leaders in dealing with North Korea on issues of nuclear crisis stability. On one axis, we have the basic assumption about the decision rationality of the North Korean leadership. On the other axis, we note whether the USA would prefer to rely on prompt or delayed launch in the face of credible, but not entirely certain, warning of nuclear attack.

From the perspective of the preceding matrix, it might appear that cells #1 and #4 produced "consistent" or "symmetrical" outcomes. That is: other things being equal, we might expect the US authorization for prompt instead of delayed launch, under plausible conditions of North Korean attack, if there were no assumption that North Korea understood and accepted the US deterrence rationality. By similar reasoning, we might expect a US preference for delayed launch if the USA assumed that North Korea understood correctly and accepted the US deterrence rationality. On the other hand, cells #2 and #3 are "inconsistent" or "asymmetrical" in raising the possibility of the US preference for delayed launch despite American doubts that North Korea understood correctly or accepted the US deterrence rationality, or the possibility of the US preference for prompt retaliatory launch even if American leaders believed that North Korea understood and accepted US rationality. (In the preceding discussion, "accepted" does not connote approval: it simply means that North Korea accepted the fact of the US deterrence being what it is, regardless North Korea's opinion of it).

<<FIGURE OMITTED>>

The matrix depicted in Fig. 3 is merely illustrative of the challenges that nuclear-armed states in Asia might face in their efforts to manage a nuclear crisis. Additional dimensions might be added to the matrix: for example, about the quality of the US intelligence with respect to North Korean intentions and capabilities. A comprehensive matrix of this sort would be as multi-dimensional as the ingenuities of policymakers, analysts, or scholars wanted to make it. However, a smaller matrix is more parsimonious in getting at the variables that matter for the discussion at hand.

Preliminary Findings and Indications

Several conclusions follow from the preceding analysis. First, strategies matter. States can guarantee larger numbers of surviving and retaliating warheads against plausible first strikes by alerting more forces sooner or by launching "on warning." However, these operational predilections may be destabilizing from the perspective of secure crisis management. On the other hand,

military planners will press for alerted and rapidly launched forces as an alternative to losing their deterrents. For example: although, apart from the USA, Russia is and will probably remain as the largest fish in the Asian nuclear pond, its long-range air forces are at risk under any conditions of day to day alert. So, too, are those of its partners and rivals in Asia.

Second, force structures also matter. Sea-based missiles are more survivable than land-based missiles. Where states can afford to build, deploy, and control a ballistic missile submarine force, it improves survivability and reduces their dependency on hair trigger alert or launch postures. An alternative to SSBN forces for smaller or less developed economies is additional reliance on cruise missiles. Cruise missiles can be based at sea on surface ships or on submarines, on aircraft or on land. They are "slow fliers" compared to ballistic missile "fast fliers" and highly survivable because of their flexible deployments and small signatures. Deployed in sufficient numbers and on diverse platforms, cruise missiles could preclude first strike vulnerability for even the smallest nuclear states. And cruise missiles are highly accurate.

Third, nuclear war is unlikely to occur by means of a surprise attack "out of the blue" absent prior political confrontation. Therefore, states' forces will, in most instances of nuclear crisis management, already be highly alerted. The most probable decision among operational postures as listed above will be that between riding out the attack and retaliating or launching on warning of attack. The results summarized in Tables 1 and 2, above, show that all states suffer a considerable penalty by waiting to ride out the attack as opposed to launching on warning of attack. However, the same tables also show that, even after riding out an attack on generated alert, each state retains numerous surviving and retaliating weapons. So: in the most likely "real world" situation of riding out an attack (with alerted forces), the smaller as well as the larger nuclear powers can guarantee unacceptable damage to any rational attacker.

Fourth, the quality of national military command and control systems matters a great deal in maintaining nuclear stability with eight, or fewer, nuclear powers in Asia. Command and control systems must provide for negative control against accidents or usurpation of authority, and for secure positive control to guarantee at least minimum or assured retaliation. Nuclear command and control systems are based on the soft power of knowledge-intensive technologies instead of the hard power of metal and mass. Disorganized or rigid command-control systems may push decision makers into unnecessary reliance on simplified options and fast triggers. Political accountability, especially during a nuclear crisis, matters just as much. Whose fingers are on the button in, for example, North Korea or Pakistan? Who is in charge? Who has the authority and control to start a war—or to end one? The answers to these questions may determine the prospects for peace in Asia.

<<TABLE OMITTED>>

Conclusions

The spread of **nuc**lear weapon**s** in **Asia** poses two kinds of **threats** to **international peace** and security. The first is that of a **deliberate** decision taken for **nuclear first strike**, either in **mistaken fear** of imminent attack, or as a **preventive war** to disable a rising and presumably threatening opponent. The second nuclear danger in Asia is that of **inadvertent escalation** growing out of a **conventional** war, and related to this, the possibility of **accidental** or **inadvertent use** of nuclear forces due to military usurpation of civil authority or **technical malfunction**.20 However, there is no reliable metric for relating the numbers of nuclear weapons states to the probability of nuclear first use. States' internal decision-making processes will drive these decisions, for better or worse. Although the international system imposes certain constraints on the behaviors of current and aspiring nuclear weapons states, the system is also the derivative of their respective national priorities and threat perceptions.

In addition, the possibility of **regional arms** races in Asia and elsewhere increases the significance of the **nuclear paradox** in American defense plan**n**ing. From one perspective, the US **nuclear mod**ernization is required, not only to deter nuclear attack or blackmail against the USA, but also to prevent **coercion** or war against its regional **non-nuclear allies**. Withdrawal of the American nuclear umbrella and the extended deterrence provided by superior US nuclear forces could increase the **risk of war** in strategic Asia. On the other hand, the USA must also pursue with Russia (and perhaps others) nuclear arms limitation and reduction agreements: otherwise, the spread of nuclear weapons to new state and possibly non-state actors will be encouraged.

1AC---Cartels---Extra

Cartels are geopolitical threats upheld by foreign actors, the aff solves.

University of Michigan 25, 04-02-2025, [John Joyce School]"No Peer Rivals," Liverpool University, https://www.liverpooluniversitypress.co.uk/doi/epdf/10.3828/9780472077397, accessed 11-2-2025 //rqli

It may be surprising for many to learn that, according to the Center for Disease Control, during the 2020–21 time frame the leading cause of death for American adults between 18 and 45 was not COVID-19, but fentanyl overdoses: this synthetic drug killed on average an American adult every eight minutes in that time span.84 And since 2021 the number of US victims of (mostly fentanyl) overdose, over 100,000, exceeds thenumber of Americans killed in action during the bloodiest year of World War II.85 Given these catastrophic statistics, it's unsurprising the US gov-ernment now recognizes international **drug trafficking**, particularly fen-tanyl, as an "**unusual and extraordinary threat** to the national security, foreign policy and economy of the United States."86 Therefore, the drugcartels that conduct most of this trafficking, and their Chinese partners who provide the fentanyl, its precursors, and increasingly financing and money-laundering assistance, must be considered a high-priority, **urgent strategic threat**. 87

The nexus between Mexican drug cartels and the CCP transforms the opioid epidemic into a national security threat, in addition to being a devastating public health and economic problem. According to Drug Enforcement Agency agent Michael Ferguson, it would not be an exag-geration to conceptualize it as a chemical weapon given its deadly impact on ordinary Americans: "Fentanyl is manufactured death. . . . Whatever can be **likened to a weapon of mass destruction and the effect it has on people**, it's fentanyl."88 Other analysts, such as Lt. Col. Nathan Rusin of the US Air Force, go even further in linking China's **unwillingness** to crack down on fentanyl to a deliberate strategy of the Chinese Com-munist Party to launch **"drug warfare"** against the United States, as part of its overall "unrestricted warfare" doctrine based on using unconven-tional and **asymmetric nonmilitary means** to **counter America's conven-tional military superiority** in the **GPC** era. In his view, "China is **pushing illicit fentanyl** into the U.S. in an effort to **destabilize, undermine and weaken** the fabric of America's social and political systems."89

While the primary motivation for this connection may indeed be financial, it is increasingly evident to both US analysts and senior mili-tary officials that the Washington-Beijing struggle for power in the era of Great Power Competition certainly shapes what some call **"a reverse Opium wa**r." 90 The author of the most comprehensive study of this con-nection so far, Fentanyl and Geopolitics: Controlling Opioid Supply from China, Vanda Felbab- Brown, is clear on the connection between the two: " , **Beijing thinks of counternarcotics collaboration as downstream from its geostrategic relations**. Unlike the U.S. government, which seeks to delink the issue from geopolitics, China views the **fentanyl crisis through the lens** of its growing **rivalry** with the United States."91

Even if the CCP were not intentionally tolerating the transfer of fentanyl to the drug cartels fueling the opioid epidemic in the United States, the connections between these two adversaries would still be worrisome enough to harm US national interests in the Western Hemi-sphere, **according to top US military officials**. 92 Testifying before Con-gress in 2021, Admiral Craig Faller, the commander of U.S. Southern Command, warned: "Two of the most significant threats are China and transnational criminal organizations. . . . Transnational criminal orga-nizations (TCOs) pose a direct threat to our national security. . . . They drive illegal migration, and they allow bad actors like China to gain influ-ence." 93 Therefore, the drug cartels pose a geopolitical threat as well because their violent activities are setting the conditions for Beijing to **advance its anti-American agenda** and **challenge US hegemony** in the **Western Hemisphere**.

Given the increasing severity of the threat posed to the US home-land and its national security by the Mexican drug cartels, unsurprisingly the US government has been searching for new ways to more effectively address it. Former secretary of defense Mark Esper's memoir even claims that President Trump inquired about a military option to destroy the car-tel labs inside Mexico.94 More recently, Congress considered legislation giving the president authority to use the US military against cartel mem-bers in Mexico, a step advocated by former US attorney general William Barr who argues that these "narco-terrorist groups are more like ISIS than like the American

mafia."95 A separate piece of legislation backed by some experts but criticized by others recommends legally designating them as foreign terrorist organizations. 96 For advocates of this measure, the old law enforcement **paradigm no longer fits** the **military advances** of the cartels: the new cartels are "composed of former Mexican spe-cial forces with U.S. military training. The Jalisco New Generation Cartel maintains an arsenal of heavy machine guns, drones, and grenades. In addition to regular massacres of Mexican civilians, the cartel is respon-sible for downing a Mexican military helicopter with a rocket-propelled grenade launcher and the grenade bombing of a U.S. embassy."97 And even if their goal is mostly to maximize profit and not political control or to conduct mass casualty attacks on American soil, the practical impact of their actions and capabilities **does indeed rise to the level** of a national security threat **worthy of countering most aggressively**, including with military force. Moreover, designating them as terrorist organizations would also allow for more effective measures to defund the fentanyl trade by giving the Treasury Department more authorities and tools.98

The United States **cannot achieve its major grand strategic goals** in distant corners of the world **unless it establishes security**, stability, and prosperity first in its own immediate neighborhood. In other words, offensive realism dictates that Washington first of all needs to effectively control **its own regional sphere of influence**: the drug cartels and their emerging relationship with China are now the biggest challenge to Washington in its own region, and hence need to be addressed with a much greater sense of urgency

1AC---Cartels---Lay

The impact of inaction is devastating.

Mark R. **Warner 23**, Senator, "Warner Calls for Increased Border Security to Stop Flow of Fentanyl from Southern Border," 10/20/23, https://www.warner.senate.gov/public/index.cfm/2023/10/warner-calls-for-increased-border-security-to-stop-flow-of-fentanyl-from-southern-border, tristan

Overdose deaths, particularly among young people, are **increasing** across our Nation. In total, the Centers for Disease Control and Prevention estimated that more than **112,000 people** died from a drug overdose between May 2022 and May 2023, with fentanyl and other synthetic opioids causing the vast majority of overdoses. Furthermore, according to a new analysis reported in September 2023, Pennsylvania, Ohio, Wisconsin, Arizona, Nevada, and Virginia were among the 37 states in which accidental drug overdoses were the largest cause of death for people under 40-years-old in 2022. In Montana, accidental overdoses of young people under 40 increased by 121% from 2018 to 2022.

The increasing rates of overdose deaths are **clearly** being **driven**, in part, by fentanyl **trafficking** across our border. From FY 2019 to FY 2022, U.S. Customs and Border Protection (CBP) seizures of fentanyl nearly tripled. So far in FY 2023, CBP has already seized over 25,000 pounds of fentanyl. In March, it was reported that CBP seized more than 21 million fentanyl tablets in the Nogales, AZ port of entry over the prior five months—more than the number of tablets seized during the entire previous year. Highlighting the complex situation that CBP must navigate when seizing fentanyl, officials have indicated that individuals are smuggling pills inside seat cushions, car batteries, metal walkers, and even hollowed-out bicycle frames. Furthermore, CBP data has shown that drugs are overwhelmingly being smuggled through U.S. ports of entry—particularly in Arizona and California—and we must do more to ensure that our CBP Officers have the funding, tools, and technology necessary to be able to stop this surge of fentanyl into our country.

Cartel violence is deadly.

Michael **Scott 24**, Member of FT's Editorial Board, "Mexico's drug cartels are thriving," Financial Times, 5/23/24, https://www.ft.com/content/fe04c6ed-73f8-4e17-852b-ce16fd6c3515, tristan

But Mexico's organised crime problem has worsened **dramatically** during the five and a half years of populist leftwinger Andrés Manuel López Obrador's presidency, security experts say, and has become so serious that it **threatens** the **country's future**. Polls show that security is a top voter concern ahead of the presidential election on June 2.

For more than a decade, the dominant drug groups have been fragmenting, generating a host of smaller splinter gangs who fight over turf. Today, the two largest and most powerful cartels, the Sinaloa cartel and the Jalisco New Generation cartel (CJNG), are jostling with smaller rivals such as the Viagras, the Squirrels and the Scorpions.

Many of the cartels have expanded into lucrative new businesses. In a 2024 report, the US Drug Enforcement Administration called the Sinaloa and Jalisco cartels "transnational criminal organisations" because they are "involved in arms trafficking, money laundering, migrant smuggling, sex trafficking, bribery, extortion, and a host of other crimes". The cartels **control more territory** than **ever before**, about a **third** of the country according to one estimate from the US military.

"There's been an **exponential deterioration**," says Manuel Clouthier, a former state deputy and businessman in the northwestern state of Sinaloa, which is home to the eponymous drug cartel. "Mexico is becoming a **failed state**."

As the cartels' economic power has grown, so has their international reach. Mexico's two top cartels now run a network of illegal activities stretching across South America that is challenging governments and alarming citizens. Battles between local affiliates of the CJNG and the Sinaloa cartel have turned previously peaceful Ecuador into one of the world's most violent countries.

The cartels source chemicals needed to make synthetic drugs such as fentanyl from China and India and have strong connections to European mafia such as the Italian 'Ndrangheta, investigators say. Anne Milgram, head of the DEA, told a US Senate committee in February last year that "the Jalisco cartel has influence through associates, facilitators and brokers on every continent except Antarctica".

In the US, Mexico's deteriorating security and flourishing drug trade have become an election issue, with Republicans calling for a tougher line. Some in the party have gone as far as calling for US military forces to nab cartel leaders in Osama bin Laden-style commando operations.

While official statistics on crimes such as murder are questioned by independent researchers, experts agree that the power of organised crime now represents a serious risk not only to the population but to business and the economy. It is one of the reasons, experts say, why the country is failing to capitalise fully on its potential to draw manufacturing away from China.

A Mexican business leader, speaking off the record because of the sensitivity of the subject, says security has deteriorated dramatically under López Obrador and that the government has played down the problem. “Nobody is talking about drug trafficking or fuel theft,” he says.

The president has painted a picture of an administration doing all it can to tackle the problem, while blaming his predecessors for creating it. He has so far avoided paying a serious political price for the deterioration. His approval rating remains at 65 per cent, according to poll aggregator Oraculus, and has barely changed in the past three years.

“The [government has] been above all trying to control the narrative,” says Falko Ernst, senior Mexico analyst at Crisis Group. “Security policy has been watered down to a PR exercise for electoral purposes.”

In reality, he adds, López Obrador’s policies have allowed criminals to continue “getting a much stronger, much more direct and much more aggressive foothold within institutions”.

Officially, security is a top priority for López Obrador. Each weekday at 6am the president chairs a security cabinet with military and police chiefs and key ministers. Twice a month his security team presents a “zero impunity” report with a blizzard of statistics covering everything from arrests to the exact number of security forces and vehicles deployed.

“Nowhere in the world is there a security cabinet where the [president] heads up daily tasks,” said Rosa Icela Rodríguez Velázquez, Mexico’s security minister, at the April 30 security briefing. Since taking office, she added, the president had presided over 1,353 security council meetings and not missed a single one.

At the start of his administration, López Obrador set out a new strategy which he called “hugs not bullets”. The idea was to tackle the root causes of crime, replace the federal police force with a new military-run National Guard and to minimise bloodshed by avoiding direct confrontation with the cartels. Instead, he appealed to cartel members to “think of their mothers”.

López Obrador intended his more peaceful approach as an alternative to Calderón’s 2006-2012 “war” and to his immediate predecessor Enrique Peña Nieto’s strategy, which had failed to contain rising murder rates.

But the president drew fierce criticism for greeting personally the mother of jailed Sinaloa cartel boss Joaquín “El Chapo” Guzmán in 2020 — something he said was a humanitarian gesture towards a woman then in her nineties.

Eduardo Guerrero, a security expert at Lantia Consultores, says López Obrador’s policy of hugs not bullets “had the . . . undesired effect of expanding the geographical presence of organised crime to new areas, precisely because the army wasn’t confronting criminals”.

Criminal groups are also interfering more brazenly in elections. This year’s campaign, which includes races for federal and state congresses, governorships and mayoralties, has been the deadliest ever. So far 36 candidates and another 45 people linked to the election have been murdered, 15 more kidnapped and dozens of others threatened, according to think-tank Laboratorio Electoral.

Another key battleground is official statistics. López Obrador’s six-year term will be Mexico’s most violent ever in terms of total murders, with more than **175,000 killed** so far. But the president has seized on figures showing a small reduction in homicides in the last three years from a record level in 2020.

Experts point out that the murder figures **do not include** the record number of people reported as missing, almost **115,000** by last year, 43,000 of whom disappeared during López Obrador’s presidency. They also note that the proportion of “crimes against life” reported as manslaughter or “other crimes” has been rising as murders fall, suggesting homicides are being reclassified.

1AC---Data Sharing

Advantage [X] is DATA SHARING.

The UK's attempt to mandate a backdoor stifles US-UK relations and data transfer.

Jones 25 [Connor Jones holds an MA from the University of Sheffield, 08-12-2025, "White House could stymie the UK's anti-encryption plans?", No Publication, https://www.theregister.com/2025/08/12/could_the_white_house_put/ DOA: 10-29-2025] Ewan

Security experts, privacy geeks, and pretty much everyone who has the faintest clue about how E2EE works knows that backdooring the likes of iMessage and WhatsApp is impossible. Data is either end-to-end encrypted or it isn't. There is no in-between.

That has not stopped multiple ruling parties in the **UK from** pushing on with anti-encryption rhetoric.

And yet, despite heavy backlash from the tech industry and beyond about the feasibility of undermining encryption, the country's lawmakers have affected change.

After it served Apple with demands to break encryption earlier this year, the tech giant threw the technically confused UK government a bone by shuttering its Advanced Data Protection iCloud feature for all Brits.

However, it seems Home Office staff are now coming to terms with the fact that the **Trump administration will block any attempt to further strongarm** Amercia's tech companies.

Insiders told the Financial Times, speaking on condition of anonymity, that the Trump administration's disapproval of the UK's plans, which the president has previously likened to Chinese-style policymaking, is the main obstacle in achieving its encryption-busting ambitions.

Officials know the US doesn't want anyone touching its tech companies. **For the UK's closest ally - historically at least - it's a firm red line.**

Should the UK indeed back down on its encryption ban ambitions, it would raise **further questions over its sovereignty** - its ability to set its own laws without having to bend the knee to the US.

There is not an abundance of cases whereby the UK's legislature has been forced to back down in the face of political pressure overseas, although some might say Huawei's removal from Britain's 5G networks – with the government issuing legal notices to vendors after US sanctions in combination with a severe diplomatic push – might be an example of this. Another semi-recent example came in 2022 concerning the UK's plan to ship asylum seekers off to Rwanda.

The EU said that plan broke international law and the European Court of Human Rights (ECtHR) issued an interim measure to stop the first deportation flights until UK courts could assess the legality of it all.

The legislation was passed by Rishi Sunak's UK government last year, but the new incoming Prime Minister Kier Starmer binned the program not long after taking office, as promised in his election run.

Ironically, the EU tabled its own regulation earlier this year to send illegal immigrants to "return hubs," one of which is rumored to be… Rwanda.

Back to the point at hand, legal experts who spoke to The Register when the UK-Apple encryption furor kicked off in January, said the UK could risk another run-in with the ECtHR if it went ahead with its encryption plans, putting it on a similar level to Russia.

Will Richmond-Coggan, partner at Freeths specializing in privacy and cybersecurity disputes, told us: "Insisting on this level of access, even with judicial supervision of the process, may well place the UK on a collision course with previous decisions made in the European Court of Human Rights, which has previously ruled (in the case of a similar attempt by Russia to broaden the scope of its domestic surveillance capabilities) that this contravened people's privacy rights."

A reminder: in its pursuit of an encryption backdoor, workaround, or however it's dressed up, the UK has been compared by its closest political ally to China, while legal experts say the potential for human rights violations would put it on par with Putinland.

That's not even considering all the other countries that are known for questionable policies to human rights, free speech, surveillance, et al.

Separate from the unwelcome company the UK would keep, such a move could lead to diplomatic difficulties with the US, with Home Office officials reportedly **concerned over how future tech deals with the US could play out.**

Tulsi Gabbard, the US's director of national intelligence, previously said of the Apple technical capability notice (TCN) that she was not made aware prior to it being issued.

She added that if the UK mandated **an encryption workaround, it would be an "egregious violation" of public privacy which could risk the data agreement held between the UK and US.**

Putting aside the potential embarrassment of the US shutting down decade-long UK policymaking efforts, privacy advocates will rejoice if the UK's attempts to bypass E2EE are foiled or otherwise buried.

It flaws the data sharing and causes privacy erosion, which turns case---only alignment solves.

Velasco 10-9 [Gwen Velasco; LLB Graduate at the City Law School, 10-9-2025, "The BluePrint Brief", No Publication, https://theblueprintbrief.com/articles/apples-encryption-fight-with-uk-reignites-over-ic/ 10-30-2025] Ewan

Commercial Impact

For Apple, the challenge is as reputational as it is legal. Disabling Advanced Data Protection for U.K. users effectively downgrades local security standards, risking customer confidence among privacy-conscious consumers and developers.

The stakes also extend beyond the U.K. U.S. lawmakers have warned that compliance with the order could conflict with the CLOUD Act, which governs cross-border data access. If Apple were to comply, it could face contradictory legal obligations under U.S. and U.K. law.

Operationally, maintaining separate encryption regimes across jurisdictions introduces technical and compliance risks. Divergent key-management systems and **data-handling rules increase the chance of system vulnerabilities**. For global tech companies, the message is clear: privacy features are no longer just product design choices, they are regulatory flashpoints.

If Apple concedes even partially, it could embolden other governments to seek similar access, leading to a patchwork of encryption standards that undermine global privacy protections.

How Legal Teams Get Involved

As Apple's appeal progresses, multiple legal and compliance functions are actively engaged:

Regulatory & Compliance Counsel

Coordinate with the Investigatory Powers Commissioner's Office (IPCO) to interpret compliance requirements while defending Apple's encryption position.

Assess potential conflicts with the Human Rights Act, GDPR, and international data-transfer rules.

Prepare reporting frameworks if encryption changes materially affect user privacy.

Product & Privacy Counsel

Collaborate with engineers to evaluate whether any design changes could introduce new legal exposure.

Conduct privacy impact assessments and ensure users are properly informed about any alterations.

Draft user communications that maintain transparency without compromising Apple's legal position.

Litigation & Risk Teams

Manage the Tribunal case and prepare for potential follow-on claims from consumers or advocacy groups.

Monitor how any ruling might set precedent for future encryption or data-access disputes.

Assess global litigation risks if the case encourages similar demands from other jurisdictions.

Government Relations & Policy Teams

Engage with U.S. and EU regulators to align approaches to lawful access and encryption.

Manage policy dialogue to preserve Apple's privacy reputation while maintaining compliance diplomacy.

Track potential reforms to the Investigatory Powers Act and anticipate long-term compliance shifts.

The plan solves---only a US backdoor mandate facilitates effective data transfer and resolves legal issues.

Salgado 25 [Richard Salgado; holds a JD from Yale University and a BA from the University of New Mexico , 7-31-2025, "Patching the U.K.'s Zero-Day Security Exploit With the U.S.-U.K. CLOUD Act Agreement", Default, https://www.lawfaremedia.org/article/patching-the-u.k.-s-zero-day-security-exploit-with-the-u.s.-u.k.-cloud-act-agreement/ DOA: 10-29-2025] Ewan

CLOUD Act Essentials

The CLOUD Act provisions at issue here were designed to reduce problems caused by U.S. "blocking statutes." Before the act, U.S. service providers could be prohibited from disclosing certain user data in response to foreign government-issued legal process, even when the request came from a rule-of-law jurisdiction in a case that all would recognize as serious and legitimate. Countries instead had to rely on diplomatic mechanisms like mutual legal assistance treaties, which are famously slow, leaving them ill-suited for some fast-moving investigations. With few realistic options, jurisdictions may turn to unilateral measures, including tactics that undermine cybersecurity.

The CLOUD Act addresses this by conditionally lifting the blocking statutes for any country that qualifies for and signs an executive agreement with the United States. To qualify, a country must demonstrate respect for civil liberties and due process, among other requirements. Once an agreement is in place, U.S. providers may honor **data requests** from that country without running afoul of the U.S. blocking statutes. As Sen. Hatch observed when introducing the bill, for the CLOUD Act to effectively address this issue worldwide, there need to be many agreements. Most of the vision that Sen. Hatch and the co-sponsors of the act enunciated remains very much in reach if the U.S. moves to enter into more agreements.

To advance the legislative goal of protecting the security of data, and encryption in particular, the CLOUD Act stipulates that an agreement "shall not create any obligation that providers be capable of **decrypting data or limitation** that prevents providers from decrypting data." Although this provision has been characterized as "**encryption neutral**" by the U.S. Department of Justice, Congress intended it to preserve the ability of providers to protect data security through encryption, as the comments of Sen. Hatch reflect.

That the provision didn't go further hardly makes it neutral. There's a like requirement in the statute that says an order issued by the foreign government under an agreement may not be used to infringe freedom of speech; that doesn't support a conclusion that the public policy of the United States is neutral as to free speech. The reported action by the U.K. seeking to require Apple to remove encryption from one of its products puts this security goal in peril.

The concerns about the security of cloud services have only grown stronger in the years since the statute was enacted, driven by an increased reliance on cloud services and a series of high-profile incidents. These include the SolarWinds supply-chain compromise (2020), the Log4Shell vulnerability affecting major cloud providers (2021), the Colonial Pipeline ransomware attack (2021), the MOVEitsoftware-as-a-service breach (2023), the so-called typhoon attacks, including the Salt Typhooncampaign in which Chinese state actors exploited Microsoft's cloud-based authentication systems to obtain communications of senior U.S. officials (2024), the U.S.

Treasury breach via a cloud vendor (2024), and the Microsoft SharePoint breach involving foreign access to Department of Defensesystems (2025), among many others.

The CLOUD Act Agreement Between the United States and the United Kingdom

Because the U.S. and the U.K. have a CLOUD Act agreement, the U.K. can issue, directly to U.S. providers, requests that comply with the terms of the agreement. The existence of the agreement means that providers may disclose the requested information without being in violation of the blocking statutes. The U.K. has availed itself of this arrangement, issuing over 20,000 requests as of October 2024.

Consequently, if the U.K. were successful in requiring a U.S. provider to remove security from a product (for example, by building in a backdoor to data that would otherwise be end-to-end encrypted), the U.K. could use the agreement to request the now-vulnerable data from the U.S. provider directly. The agreement itself, however, includes a safeguard mechanism that allows the U.S. to protect data from foreign efforts to undermine the security and privacy protections provided by American companies.

Specifically, the agreement has a provision that either the U.S. or the U.K. can invoke to resolve concerns about implementation or disputes, and if not resolved to its satisfaction, to exclude categories of requests from the scope of the agreement. The pertinent provision is Article 12.3:

In the event that the Parties are unable to resolve a concern about the implementation of this Agreement or a dispute, either Party may conclude that the Agreement may not be invoked with respect to an identified category of Legal Process, including Legal Process that are issued on or after a particular date. Notification of that conclusion must be sent by the Designated Authority of the Party that has so concluded to the Designated Authority of the other Party. The notified Party shall not invoke the Agreement with respect to any Legal Process within the identified category upon receipt of such notification. Such a conclusion may be revoked at any time, in whole or in part, by the Party that reached the conclusion through a notification of the revocation to the other Party's Designated Authority. Any data produced to the Issuing Party shall continue to be subject to the conditions and safeguards, including minimization procedures, set forth in this Agreement.

This open-ended provision gives either the U.S. or the U.K. the opportunity to exercise oversight over the other's use of the agreement. A party may identify a "concern" that it believes has arisen in the course of implementation, or the existence of "a dispute." In this instance, there already is substantial evidence in bipartisan congressional and executive statements of the level of U.S. disquiet about the U.K. order to Apple.

Invocation of Article 12.3 as a Stopgap Measure

The U.S. thus may invoke Article 12.3 of the agreement to determine, either by agreement with the U.K. or through a unilateral conclusion, that the U.K. may not use the CLOUD Act agreement to seek data from any U.S. provider on which it is attempting to impose, or has imposed, restrictions on security or privacy features, or mandates that the provider build capabilities for the U.K. to surveil customers. **U.K. law enforcement and intelligence agencies therefore could benefit from surveillance capabilities mandates only to the extent that such obligations are imposed on American companies by U.S. law.**

Exercising Article 12.3 in this manner ensures that the U.K. could not circumvent the U.S. democratic process or override the considered choices made by elected representatives in the United States by requiring those companies to adopt additional or broader surveillance capabilities beyond what U.S. law mandates. Such an understanding could be memorialized in a diplomatic note, acknowledged by the United Kingdom, and forming an integral part of the agreement.

Effective data sharing resolves cooperation.

Byman 25 [Daniel Byman is a lawyer and researcher, 3-6-2025, "Improving U.S. Intelligence Sharing With Allies and Partners", Default, https://www.lawfaremedia.org/article/improving-u.s.-intelligence-sharing-with-allies-and-partners, DOA: 10/31/25] phab

The Trump administration's recent decision to cut off intelligence sharing with Ukraine will get less attention than its halting of military aid, but it will also be consequential. If anything, the United States should be increasing intelligence cooperation not only with Ukraine, but also with other key partners.

Intelligence sharing is **a cornerstone of U.S. efforts to ensure its own security and that of key allies and partners.** Effective sharing enhances strategic coordination, enables timely responses to threats, and strengthens trust between nations. Despite its importance, intelligence sharing does not live up to its

potential. As Sean Corbett and James Danoy—former senior British and U.S. intelligence officials, respectively—have written, "With few exceptions, and despite the best of intentions, **intelligence sharing is uneven**, remains the exception rather than the norm, and the prospect of simultaneity at the point of need is remote." Drawing on a larger research project that drew heavily on interviews with U.S. and allied officials and experts, this piece critically examines the current state of U.S. intelligence sharing, identifies key challenges, and proposes solutions to improve the effectiveness of these partnerships.

As a former head of the U.K. Secret Intelligence Service put it, intelligence is "a team sport." The U.S. intelligence community operates within a complex web of alliances, including the Five Eyes (composed of the United States, Australia, Canada, New Zealand, and the United Kingdom). The Five Eyes, however, are an exception: Bilateral cooperation is the preferred form of intelligence liaison, primarily for security reasons. The more widely information is disseminated, the more likely it is to be revealed through spying, media leaks, or other unauthorized disclosures.

Intelligence relationships help preempt threats ranging from terrorism to cyber and conventional war. Intelligence collaboration allows for **resource pooling, which reduces individual states' intelligence burdens.** Sharing also lays the groundwork for shared threat perceptions, which in turn makes cooperation and planning easier. Sharing also expands collection opportunities. For example, some partner states have a presence in countries like Iran, which gives them intelligence reach where it is denied to any official Americans. Further, intelligence-sharing agreements reinforce alliances and serve as instruments of diplomatic engagement, signaling commitment and trust.

The impact of sharing failures, though difficult to measure, can be felt in several pernicious ways. Allies and partners may be slow to realize dangers posed by revisionist powers such as China, Russia, and Iran. **Advanced planning based on varied intelligence assessments can hinder cooperation in a crisis.** As one European official told me, "All plans depend on intelligence. Bad intelligence means bad plans." An ineffective division of labor may cause collection and analysis to suffer from both gaps and overlap. Information may be shared too slowly to matter, especially in a rapidly changing situation. Intelligence sharing can bolster overall diplomacy between allies; without it, an important pillar of that relationship is weakened.

Intelligence sharing, however, is governed by a labyrinth of policies, laws, and bureaucratic frameworks that can hinder timely information exchange. U.S. prioritization in both collection and sharing is often unclear, confusing both U.S. and allied officials. The classification system, such as the U.S. marking of "NOFORN" (not releasable to foreign nationals), often prevents intelligence dissemination, even to close allies. The United States, as one U.S. official put it, "does not have any info sharing policies at all. It has information security policies and information sharing exceptions to these policies." In addition, the system itself has uneven and confusing standards and much harsher penalties for over-sharing than for under-sharing, making the default to NOFORN even more likely and "wild overclassification" common, as one U.S. official told me.

Trust is the bedrock of intelligence collaboration. Henry Kissinger once remarked that "there is no such thing as friendly intelligence agencies. There are only the intelligence agencies of friendly powers." Beyond spying, concerns over leaks, misuse, or politicization of shared intelligence can also erode trust. The Snowden disclosures in 2013, for example, strained relations between the U.S. and some of its closest allies, highlighting vulnerabilities in intelligence handling. Another problem is the global nature of U.S. interests: European officials worry that the United States will focus too much on Asia, and Asian partners worry the United States will focus too much on Europe.

Intelligence sharing is increasingly dependent on secure and interoperable technical systems. However, technological disparities among allies, coupled with differing cybersecurity standards, create significant interoperability challenges. As one Five Eyes official told me, "Just because we have an intelligence sharing agreement doesn't mean we have intelligence sharing systems." The absence of standardized data-sharing protocols and **encrypted communication systems** further exacerbates inefficiencies in real-time intelligence dissemination.

Differences in intelligence cultures and bureaucratic structures across nations complicate collaboration. While the U.S. intelligence community operates under a relatively centralized framework, despite the bureaucratic weakness of the director of national intelligence, other countries have even more balkanized systems, and many services are politicized. Divergent priorities and intelligence methodologies can hinder seamless integration and coordination. Sir Stephen Lander, the former director general of the U.K. Security Service, remarked in 2004 that some countries "collect haystacks and store them, while others collect hay and store needles, while others again only ever collect needles and not very many of them. The risk of sharing haystacks with needle keepers is that they would not be able to use the material effectively or would be swamped."

Strained UK-US bilateral relations embolden Russia.

Financial 25 [Financial is a news organization, quoting Angela Stent, who holds an MA and PhD from Harvard University, a MSc from the London School of Economics, and a BA from Girton College ,

4-17-2025, "The UK-US "Special Relationship" in Crisis", FINCHANNEL, https://finchannel.com/the-uk-us-special-relationship-in-crisis/125236/uk-politics/2025/04/ DOA: 10-30-2025] Ewan

Expert Insight: Angela Stent, a senior fellow at the Brookings Institution and Russia expert, argues that "Putin sees a fragmented NATO as a strategic win." **She notes that Russia benefits when allies like the UK, which hosts critical US military bases** (e.g., RAF Lakenheath and Mildenhall), question American reliability. A weakened US-UK security partnership could reduce the effectiveness of these bases, which are vital for NATO's rapid response capabilities in Europe. Stent emphasizes that Russia's disinformation campaigns amplify transatlantic discord, portraying the US as an unreliable partner to European audiences.

Russian Gains: A **fractured NATO emboldens Russia to pursue aggressive actions** in Eastern Europe, particularly in Ukraine and the Baltics. With the UK—a staunch NATO advocate and major military contributor—potentially sidelined by tensions with the US, Russia faces less coordinated Western resistance. For example, the UK's leadership in training Ukrainian forces **and supplying** weapons like Storm Shadow missiles could falter if US-UK intelligence-sharing or logistical cooperation weakens.

Russia can exploit Europe's security anxieties by offering bilateral energy or trade deals to individual nations, bypassing EU frameworks. For instance, Russia has historically used gas exports to cultivate influence, as seen with Germany's Nord Stream projects before 2022. **A distracted UK**, focused on navigating US tariffs and EU relations, is less able to counter such Russian overtures. Additionally, Russia's cyberattacks and hybrid warfare tactics—such as disinformation campaigns targeting European elections—fac

Russia can position itself as an alternative trade partner for European nations desperate to mitigate economic fallout. For example, Russia's discounted oil and gas exports, redirected from Europe to Asia since 2022, could be offered to select European countries willing to weaken sanctions. The UK, facing domestic pressure to stabilize its economy, might indirectly benefit from European neighbors softening their stance on Russia, reducing the collective Western economic front. Moreover, Russia's propaganda can amplify anti-American sentiment in Europe, framing the US as the source of economic woes and Russia as a pragmatic partner.

A weakened US-UK front on Ukraine allows Russia to dictate terms in negotiations, potentially securing territorial gains or a frozen conflict that preserves its influence. Russia also benefits from reduced Western military aid to Ukraine, as the UK's resources are stretched and US commitment wanes. For instance, if US-UK coordination on arms supplies like ATACMS missiles or Challenger tanks falters, Ukraine's battlefield capabilities diminish, giving Russia a military edge. Additionally, Russia's domestic propaganda can portray transatlantic discord as evidence of Western decline, bolstering Putin's narrative of Russian resilience.

Russian aggression causes great power war.

Lorenz 22 [Wojciech Lorenz, PhD, analyst for the Polish Institude of International Affairs, January 2022, "Deterrence in the Baltic Sea Region A View from Poland," The Polish Institute Of International Affairs, The Hague Centre for Strategic Studies, https://hcss.nl/wp-content/uploads/2021/12/04-Deterrence-in-the-Baltic-Sea-Region-HCSS-2022.pdf/ DOA: 10-31-2025] Ewan

Although Russia's aggressive policy can be perceived as intimidation tactics, it has also increased the risk that Moscow could decide for open confrontation with NATO. Large- scale exercises could be used for political signaling to intimidate and divide the Alliance but they also increase the risk of aggression by shortening warning time for military attacks and offering convenient cover for offensive operations12. Under the pretext of acting in self-de- fense, Russia can move forces to NATO members territory and by threatening other allies with long range dual-capable weapons (for example, Kalibr cruise missiles and Iskander ballistic missiles), divide NATO and discourage it from the attempts to regain control over the lost terri- tory13. Hybrid strategies, which so far have been kept under the threshold of open confronta- tion, could facilitate surprise aggression and quick escalation, delaying or weakening NATO's response and political will to re-establish the status quo ante. In such case, Russia would be negotiating from the position of strength and could demand that NATO members accept new legally binding pan-European or regional security arrangements in exchange for the end of hostilities. In this aspect, Russian threat towards NATO differs from the threat posed by China to Taiwan. While China's goal is to take control over Taiwan by political means or through mili- tary force, Russia's goals do not necessarily require the occupation of NATO's member state territory. It may be enough for Russia to provoke limited conflict, threaten the Alliance with the escalation and use it as a bargaining chip during the negotiations on the political resolution of the crisis. There are, however, important similarities. Both states may try to establish control over the areas perceived as crucial for their security (Ukraine, in case of Russia, and the South China Sea, in case of China) and when not met with strong resistance they can feel encour- aged to use force to achieve their ultimate goals.

The decision by Russia whether to use force against a NATO member would be influenced by a number of operational and political factors, which include the assessment of NATO's military capabilities necessary to defend Allied territory and to fight a war under the threat of escalation up to nuclear level. Equally important would be the perception of US commitment to NATO and the assessment of the Alliance's political cohesion, which might be decisive for allies' determination to launch a collective defense mission. Russia's calculations could be, for example, influenced by the US engagement in a conflict with China in the Indo-Pacific, especially if the US would be unable to commit sufficient potential to support NATO collective defense mission, whereas NATO would be divided over the form and scale of support for its US ally14 .

The Baltic Sea region offers Russia a number of options to increase tensions under the threshold of open conflict, test NATO's resolve, provoke a limited war with NATO and threaten the Alliance with further escalation. Baltic States have some Russian-speaking minorities, which could be used for provocation and exploited as a pretext for aggression. Relations with Belarus makes it possible for Kremlin to use Belarusian security services as a proxy against NATO states such as Poland, Lithuania and Latvia. Russia can use Belarusian territory and Kaliningrad Oblast, a heavily militarized exclave, to close the so-called Suwalki Gap - a corridor leading from Poland to the Baltic States, cutting them off from NATO reinforcements. The mixture of defensive/offensive capabilities placed in Belarus and Kaliningrad could be used to create an anti-access/area denial zone (A2/AD) over the Baltic States and Poland increasing the risks and costs for the Alliance to launch a collective defense operation15 .

Russia also demonstrates that is has the ability to fight with NATO in different regions from the High North, through the Baltic Sea and the Black Sea regions to the eastern Mediterranean. **Such ability is necessary for Russia to defend itself but is also used during exercises to signal that Russia has the ability to fight a full-scale war in many regions at the same time**. It also offers the opportunity to provoke conflict in a region different than the Baltic Sea area, to achieve strategic surprise.

After the annexation of Crimea, Russia augmented its A2/AD capabilities in the Black Sea, and tries to take control over Ukrainian territorial or international waters and to deny NATO access to the Black Sea basin16. Russia could provoke crisis by attacking a NATO ship, present it as an action in self-defense and, should the Alliance decide to reassure allies and deter Russia by strengthening its presence in the region, use it as a pretext for further escalation, with a viable option of troops landing on NATO shores. Similarly, as in the Baltic Sea region, Russia would use hybrid strategies to influence a threat perception of NATO populations and deci- sion-makers, and exploit political divisions in NATO states and across the Alliance to delay or weaken NATO's response. **It would use propaganda and disinformation, cyber-attacks and military signalling**. Demonstration of long-range precision strike capabilities, which are able to hit target across Western Europe, supported with nuclear signalling (overflights of nuclear capable bombers, tests of ballistic missiles) would send a signal that Russia is prepared to escalate conflict and, should it face a defeat, it could contemplate the use of nuclear weapons to de-escalate it.

CSAM

1AC---CSAM---Lay

Platforms are increasing encryption, which decks efforts to combat CSAM.

Steven **Wasserman 24**, President of the NAAUSA, "Why end-to-end encryption is the next battlefield for tech justice," The Hill, 2/22/24, https://thehill.com/opinion/technology/4482935-why-end-to-end-encryption-is-the-next-battlefield-for-tech-justice/, tristan

The Senate Judiciary Committee came head-to-head with an all-star lineup of tech titans recently to discuss the widespread proliferation of child sexual abuse material (CSAM) on their platforms. But while senators raised a variety of concerns, end-to-end encryption received almost no airtime, with only one senator and one social media company raising the issue.

Despite the lack of attention, **encrypted messaging** remains the **single greatest barrier** to law enforcement action against those who commit online crimes.

Social media **companies** are **increasingly** adopting end-to-end **encryption** to provide better privacy protection to users. Indeed, law enforcement has praised end-to-end encryption to prevent identity fraud and theft. But too often the technology translates to a **complete lock-out** of law enforcement.

A company can effectively block law enforcement from obtaining evidence, even by court-ordered wiretap or search warrant. This **obscures** law enforcement's ability to **prevent** and **prosecute** crimes — particularly those crimes that are frequently committed on social media and messaging apps, such as child sexual exploitation, terrorism-related offenses and drug trafficking.

Even Discord CEO Jason Citron acknowledged this risk during the hearing, saying end-to-end encryption "blocks **anyone** including the platform itself from seeing users' communications."

"It's a feature on dozens of platforms but not on Discord. That's a choice we've made," he said. "We don't believe we can fulfill our safety obligations if the text messages of teens are fully encrypted because encryption would block our ability to investigate a serious situation, and when appropriate report to law enforcement."

It is true. If the social media companies themselves cannot access encrypted data, it is **impossible** to believe law enforcement could gain access to criminal evidence.

Nonetheless, in December, Meta announced its decision to make end-to-end encryption the default setting across its messaging platforms. This decision comes among widespread concern by law enforcement and victim advocacy groups that the move will **severely** diminish the ability of law enforcement to **investigate** and **prevent** dangerous and violent offenses, such as **C**hild **S**exual **A**buse and terroris**M**.

An international alliance of 15 law enforcement agencies dedicated to addressing global threats from child sexual abuse, named the Virtual Global Taskforce, which includes the Federal Bureau of Investigation and Immigration and Customs Enforcement's Homeland Security Investigations, described Meta's decision as a "purposeful design choice that degrades safety systems and weakens the ability to keep child users safe."

The taskforce shared the story of David **Wilson**, one of the most **prolific** child sexual abuse offenders the UK's National Crime Agency has ever investigated, who used Facebook to contact and groom **thousands** of children. He created fake profiles pretending to be a teenage girl to manipulate victims into sending him sexually explicit material of themselves. Victims were sometimes blackmailed into abusing their friends and siblings, and were frequently traumatized by the experience.

The UK National Crime Agency was able to successfully prosecute Wilson because law enforcement was able to **access** the evidence contained within over 250,000 messages through Facebook.

End-to-end encryption makes investigations like these all but **impossible**. Still, Meta CEO Mark Zuckerberg acknowledged during the hearing that minor users have access to encrypted messaging across their various platforms, such as WhatsApp.

Previously, Meta had been one of the largest reporters of CSAM material online. But like Google and Apple, who previously routinely provided law enforcement access to data on mobile phones when under a court-ordered search warrant, the move toward encryption has locked out law enforcement.

Meta's response? According to its safety strategy, "[L]aw enforcement may still be able to obtain this content directly from users or their devices." Essentially, Meta expects law enforcement to request data on criminal activity from the criminals themselves.

Meta, along with other social media companies in attendance at the hearing, claim they are using artificial intelligence and other technology innovations to identify and remove predators online. While these are commendable steps, they are not a substitute for criminal prosecution.

Ultimately, public safety should not be entrusted to a private company. Law enforcement **must** have a process for obtaining **lawful access** to **encrypted data**.

That allows predators to go free.

Jennifer **Daskal 22**, Former Director of the Tech, Law, and Security Program at American University, Professor of Law, Former Deputy Homeland Security Advisor, "Protecting Children in the Age of End-to-End Encryption," 10/27/22, https://www.american.edu/wcl/impact/initiatives-programs/techlaw/projects/protecting-children-in-the-age-of-end-to-end-encryption.cfm, tristan

End-to-end encryption **obscures** the content of communication among **all parties**—the child, the trafficker, and the demand-side offender. When the child is party to the communication, that may provide an opportunity to obtain the content. However, a strong majority (**88%**) of respondents to the aforementioned survivor survey reported they would **not** want their trafficker prosecuted,45 which means they may **not** be willing to **cooperate** with law enforcement. In-person interventions may therefore provide some of the more promising solutions to combat this pattern of harm.

Encryption prevents content moderation.

Jennifer **Daskal 22**, Former Director of the Tech, Law, and Security Program at American University, Professor of Law, Former Deputy Homeland Security Advisor, "Protecting Children in the Age of End-to-End Encryption," 10/27/22, https://www.american.edu/wcl/impact/initiatives-programs/techlaw/projects/protecting-children-in-the-age-of-end-to-end-encryption.cfm, tristan

Measuring the global scope of child sexual exploitation and abuse with accuracy is extraordinarily difficult due to variations in definitions and data collection practices across jurisdictions.12 Here is what can be stated with certainty: in 2021, NCMEC13 received over **29 million reports** of suspected child sexual exploitation, **up** from 21.7 million reports in 2020, and more than 10 times the number received a decade prior.14

This dramatic increase in reports is not exclusively due to a concomitant increase in hands-on abuse or distribution of CSAM (although increases in these activities may account for some of the change). Instead, this increase is likely due, in part, to ESPs adopting **highly efficient detection** tools.15 PhotoDNA, a CSAM detection tool that relies on "**perceptual hashing**" technology, was developed in 2009 and has been **widely adopted** throughout the tech industry.16 ESPs use this program, as well as programs like it, to automatically **scan content** on their platforms **to detect CSAM**. This method has proved extremely **accurate**, **reliable**, and **fast**.17 It is this process that Meta has used with Facebook Messenger and that is credited for the large amount of **reporting** by Meta to NCMEC; in 2021, Facebook made 22.1 million reports (out of the 29.2 million received total from ESPs) to NCMEC.18

In end-to-end **encrypted** environments, ESPs **cannot detect** and **report** CSAM using perceptual hashing techniques. As more and more tech companies implement end-to-end encryption, the volume of **reports** to NCMEC will likely drop **dramatically**. **Regulations** in Europe provided a **realworld test case** to examine the impact on reporting when hash-matching methods are disrupted. In December 2020, the ePrivacy Directive in the European Union (EU) went into effect and, for a time,

limited ESPs' ability to use hash-scanning technology to **detect** CSAM. NCMEC examined EUrelated reports submitted by ESPs in the weeks before and after the directive went into effect and found that the number of reports deceased by **51%** in the first six weeks.19

That prevents life-saving action.

NCMEC ND, Nation's largest and most influential child protection organization, "End-to-End Encryption," National Center for Missing & Exploited Children, https://www.missingkids.org/theissues/end-to-end-encryption, tristan

End-to-end encryption is a term used to describe blocking or preventing any third-party recipient from **viewing**, **reading** or becoming aware of information that one individual has sent to another. In response to growing concerns about online data security, many technology companies are adopting this strategy with potentially dire circumstances.

The use of end-to-end **encryption** would prevent the companies or any third-party from detecting **illegal** activity occurring on their platforms, including the activity of people who use the internet to perpetuate online demand for graphic sexual abuse material of children.

We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, **millions** of incidents of abuse will remain **hidden**, leaving these young victims **without** any **help** or **protection** from these horrific crimes.

CSAM is devastating. Independently, encryption enables widespread distribution.

Komal **Mishra 24**, Researcher, "Hidden Horrors: Comprehensive Reports and Statistics on CSAM," SSRN, 7/18/24, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4898385, tristan

Addressing Child Sexual Abuse Material (CSAM) is crucial due to its **profound** and **lasting impact** on victims, the **pervasive** nature of its distribution, and the broader societal implications. Tackling this issue involves **protect**ing vulnerable children, **prevent**ing future abuses, and holding perpetrators **accountable**.

Victims of CSAM suffer **severe** and **long-lasting** psychological, emotional, and physical harm. The abuse depicted in CSAM is not a one-time event; the circulation of these materials perpetuates the trauma. Victims often experience **anxiety**, **depression**, and post-traumatic stress disorder (**PTSD**) due to the knowledge that images of their abuse are permanently **accessible online**. This ongoing victimization can hinder their ability to **recover** and lead a normal life.

The prevalence of Child Sexual Abusive Material (CSAM) is a pressing global issue, reflecting the widespread and growing nature of child exploitation and abuse. While precise figures are difficult to ascertain due to the clandestine nature of these activities, various studies, reports, and statistics shed light on the scope of the problem.

Internet and Dark Web: The internet, especially the dark web, has **significantly increased** the accessibility and distribution of CSAM. Offenders use **encrypted communication** and anonymous browsing **to share** and trade abusive material.

Social Media Platforms: Social media and instant messaging apps have become channels for the rapid dissemination of CSAM, often through covert groups and networks.

Global statistics of CSAM

In 2022, 64.5% of reported CSAM websites were in Asia, 5.2% in Europe, 8.3% in North America, and 10% in Africa.

Between 2020 and 2022, India reported 13.1 million pieces of CSAM website content, the Philippines reported about 7 million, and Pakistan reported 5.3 million.

In 2023, the National Center for Missing and Exploited Children (**NCMEC**) received over **36 million** reports of suspected child sexual exploitation to CyberTipLine and over 104 million CSAM-related files from registered Electronic Service Providers.

Factory Farming

1AC---Factory Farming

Advantage [x] is FACTORY FARMING.

The AFF enables hacktivism.

Vincent '16 [Roland Vincent; Animal Rights Activist; 01-03-2016; "Hacktivism. The Future of Direct Action?"; Armory of the Revolution; https://armoryoftherevolution.wordpress.com/2016/01/03/hacktivism-the-future-of-direct-action/; accessed 10-19-2025] leon

Cyber hacktivists save **millions** of animals! This is a great and timely idea.

<<TEXT CONDENSED NONE OMITTED>>

As noted in previous blogs, animal rights activists have not made enough progress using other means. The big organizations in this country and abroad have decried animal abuse for years, and the Internet has disseminated their information. YouTube videos reveal levels of human cruelty to animals that is sickening and could never be adequately conveyed in the written word. PETA, founded in 1980, emphasized animal rights over welfare and asserted that animals are not ours to exploit. HSUS added more rights messages to its previous welfare orientation. The most neglected and abused animals of all–farm animals–finally got more notice: Farm Animal Reform Movement was founded in 1981, Farm Sanctuary in 1986, Compassion Over Killing in 1995, Mercy for Animals in 1999. The list continues to grow and includes sanctuaries and shelters for domestic and wild animals. So advocates dispensed leaflets, wrote letters, promoted veganism, protested, and rescued. The Animal Liberation Front's dedicated activists went further and broke the law in their raids to free animals and destroy equipment and records, ruining months, perhaps years, of research data. However, they had to work fast to avoid being caught. They were often limited by terrain, security measures, and escape routes. When apprehended, they went to prison. What have we to show for it all? We have shelters still filling with doomed kittens and abandoned grey-muzzled dogs; sanctuaries agonizing over which desperate horse or tiger they can afford to save; transport trucks with their cargo of misery pulling onto freeways every day; slaughterhouse workers prodding billions of terrified victims to the hell of the kill floor; bureaucrats deciding which wild animals will live or die.

<<LINE BREAKS CONTINUE>>

So cyber terrorism should be **the step**. Hackers could target the **companies** and **individuals** who deserve to be punished the most, such as the **Big-Ag** complex. They could destroy **account information**, delete payrolls, put embarrassing interoffice memos on the Internet, and perhaps shut down **assembly lines**. Profits would fall and jobs would be **lost**. The pain would fall on CEO and worker alike, as all are complicit in the abuse.

Hackers could conduct attacks from **virtually anywhere** in the world. They would have no fear of security guards or cameras. They would not have to watch the clock or worry if they could run fast enough. They could throw their laptops and flash drives into bags and escape from one country to another as the need arose.

The hackers could also take a lesson from **SHAC** (Stop **Huntingdon** Animal Cruelty). This group conducted protests against Huntingdon Life Sciences, a **large business** who sold animals for **experimentation**. SHAC targeted employees and family, but they also aimed at secondary targets, as well, such as **business partners**, **insurers**, even caterers and **cleaners**. When those companies tired of the **protests** and **severed ties** with Huntingdon, its **stock tumbled**. Do we see possibilities here? Lots of opportunities?

Attacks work.

Creswell '21 [Julie Creswell; Business Reporter Covering the Food Industry; 06-03-2021; "Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business"; The New York Times; https://www.nytimes.com/2021/06/01/business/meat-plant-cyberattack-jbs.html; access at https://archive.ph/DYjw6; accessed 10-18-2025] manan + leon

A **cyberattack** on the world's largest **meat processor** forced the shutdown of nine **beef plants** in the United States on Tuesday, according to union officials, and disrupted production at poultry and pork plants. The **attack** could upset the nation's **meat markets** and raises new questions about the vulnerability of critical American businesses.

The company, JBS, said the majority of its plants would reopen on Wednesday. But even **one day's** disruption at JBS could "significantly **impact**" wholesale **beef prices**, according to analysts at Daily Livestock Report.

The **breach** at JBS was a **ransomware attack**, the White House said — the **second** recent such attack to freeze up a critical U.S. **business operation**. Last month, a ransomware attack on Colonial Pipeline, which transports gas to nearly half the East Coast, triggered gas and jet-fuel shortages and panic buying.

Factory farms are dependent.

Yang ‘25 [Xufei Yang; Assistant Professor, SDSU Extension Environmental Quality Engineer; 06-24-2025; "Protecting Your Data: The Role of Authentication and Encryption in Agricultural Cybersecurity"; South Dakota State University Extension; https://extension.sdstate.edu/protecting-your-data-role-authentication-and-encryption-agricultural-cybersecurity; accessed 10-18-2025] leon

Before we dive in, here are the different types of data used in **farming**:

Farm Operation Data: Includes **information** on crop yields, soil health, irrigation schedules, **livestock** weight, and feed consumption, helping farmers make better decisions.

Sensor and IoT (Internet of Things) Data: Comes from technology like weather stations, drones, water meters, and livestock trackers, providing real-time monitoring of farm conditions.

Financial Data: Includes data related to all **financial transactions** of the farm, such as loans, debts, assets, profitability, and account balances. It contains valuable information about the financial position of the farm.

Personal Data: Involves details about employees, customers, and other individuals connected to the farm, important for workforce management and customer relations.

These data are crucial for **automating** farm operations, managing finances, and **maintaining business** relationships. However, if stolen or hacked, they can lead to serious disruptions, financial losses, or even identity theft. Data protection is essential to keeping farms running smoothly and securely.

<<TEXT CONDENSED NONE OMITTED>>

What is Data Authentication? Data authentication ensures that information is real, trustworthy, and comes from the right source. It also ensures that the data has not been changed or tampered with during storage or transmission. In the digital world, authentication is widely used to protect data integrity. Below are several data authentication measures used in agriculture. Passwords and multi-factor authentication Today, passwords are required to verify user identity on almost all modern agricultural equipment and software. This includes farm management platforms, cloud servers, GPS-guided machinery, drones, smart controllers in livestock barns, and RFID systems. With password-based authentication, users enter a username and password to log in. The system then converts the password into a secure digital format and checks if it matches the stored record. If it does, access is granted. Using a strong password is crucial for keeping your account and data secure. However, passwords alone only prove that someone has the right login details. They do not confirm who is actually using them. Hackers who steal a password can easily access farm equipment and software, putting valuable data and operations at risk. Multi-Factor Authentication (MFA) is becoming more widely used to address this issue (Figure 1). A sketch diagraming different factors used for multi-factor authentication, including something you know, are, and have. For a detailed description, please call SDSU Extension at 605-688-4792. Figure 1. Multi-factor authentication for secure login. The figure illustrates the use of at least two factors (who you are, what you have, and what you know) to enhance login security. (Courtesy: Sketchplanations, CC BY-NC 4.0) MFA is a security protocol where the user must provide two or more pieces of evidence to prove who they are when logging in. Besides your password, you might have to enter a one-time code sent to your email or phone, confirm a login request on a phone app, or use a fingerprint or face scan. Digital signatures and certificates A digital signature is a unique “fingerprint” code attached to data, verifying that it comes from the intended device and has not been changed. It helps protect agricultural data, prevent fraud, and ensure that farming and supply chain records remain trustworthy. The signature is created by converting the original data (including device details and readings) into a short, fixed-length code called a hash, which is then locked using a private key. When someone receives the data, they unlock the signature using a public key and compare it to a newly generated hash of the received data to ensure it matches. This makes it nearly impossible for anyone to tamper with the data without being detected. Examples of digital signatures in agriculture include: Data transmission: Data from soil moisture sensors is digitally signed to ensure that farmers receive and utilize data from a trusted sensor, and no one has changed the data before it reaches them. Record validation: Modern farm machines can automatically keep logs of what they do, such as GPS locations and seeding rates. These records can be digitally signed to make sure no one changes them later. This helps with keeping trustworthy records and meeting regulations. Authentication of Ag Internet-of-Things (IoT) devices. Each device in an Ag IoT network, such as drones, weather stations, and soil sensors, is assigned a digital certificate to ensure only approved devices can connect to the network and share data. This helps keep the system secure from fake data or hackers. Verification of user identity. On shared agricultural data platforms, each user is given a digital certificate stored on a smart card or similar device. This helps ensure that only authorized people can access the system and makes it easier to track who does what. A digital certificate is like an online ID card issued by a trusted organization to prove who someone or something is in a digital farming system. It includes a set of information such as the name of the person or device, a public key, who issued the certificate, when it expires, and a unique serial number. While similar to digital signatures, digital certificates involve a more complex implementation. They play a crucial role in verifying identities and ensuring that only authorized users and devices can access sensitive agricultural data. Role-based access control (RBAC) RBAC allows different groups of users, such as administrators, employees, or guests, to have different levels of data access in a digital farming system. This means each person can only see or do what is needed for their assigned role within an organization or supply chain, helping keep the system organized and safe. Below are some examples: Livestock farm management software: Workers can only see and update the information they need for their daily work, such as tracking livestock weight, feed use, health checks, and vaccinations. Only the farm owner or manager can have full access, including sensitive information such as financial data. Ag IoT systems: In a smart irrigation system with devices like weather stations, soil sensors, pumps, valves, and water meters all connected online, RBAC helps control who can do what. For example, only the farm manager using the office computer can issue commands or change system settings, while others can only view the data. Supply chains: In a meat supply chain system, people like livestock caretakers, processing plant workers, truck drivers, retailers, and inspectors each have access only to the information and tools necessary for their specific jobs. This helps ensure traceability and food safety compliance from farm to fork. For example, a retailer can see the full history of where the meat came from, but they cannot change any of the records. What is Data Encryption? Digital padlock over a circuit board, representing data encryption. (Courtesy: Jaydeep Joshi, Pixabay)

<<LINE BREAKS CONTINUE>>

Data **encryption**, a more advanced form of ‘secret code’ or ‘ciphers’, is the process of transforming data using a secret key into a coded format that no one can understand unless they have the correct key to unlock and read it. Encryption alone does not stop hackers from **accessing data**, but it makes the data **unreadable** and **useless to them**.

<<TEXT CONDENSED NONE OMITTED>>

There are two main ways to keep data safe using secret keys. The first way is like using the same key to lock and unlock a door. This is called symmetric encryption, where the same secret key is used to both encrypt and decrypt the data. The second way uses two different keys: one to encrypt the data (called the public key) and another to decrypt it (called the private key). This is known as asymmetric encryption and is a bit like having a mailbox: anyone can drop a letter in (encrypt it), but only you have the key to open it (decrypt it). Both methods are widely used to keep information secure in the real world. So, what exactly is a secret key? It is a string of letters, numbers, and/or symbols used by an encryption algorithm to transform data. Consider the algorithm as a set of rules for locking and unlocking information, and the key tells it exactly how to do that. Like a strong password, a longer and more complicated key makes it harder for someone to break in. However, stronger keys may take more time and computer power to use. Most importantly, the key must be kept secret. If hackers get access to it, they could decrypt and read your sensitive information. Common Encryption Algorithms For simplicity, only two commonly used encryption algorithms are discussed here: SSL/TLS (Secure Sockets Layer/Transport Layer Security) For instance, you have probably noticed some websites start with https:// instead of just http://. That extra “s” means the site is using SSL or TLS to keep your connection secure and protect your information as you browse. With SSL/TLS, the data transmitted between a web server, like SDSU Extension, and a browser on your computer or phone is encrypted, so that no one else can spy on what you are doing. AES (Advanced Encryption Standard) AES is a symmetric encryption method that uses the same key to encrypt and decrypt data. It is widely used to keep data safe during transmission between farm devices, like sensors and controllers, and their associated computers or software programs. AES works by breaking data into fixed-sized blocks and encrypting them using keys of different lengths. Like passwords, the longer the key, the stronger the protection. Example: How AES helps keep data secure Imagine a soil probe in the field sends a real-time reading of “SP1 62.5 43.8%”. Here, SP1 is the sensor ID, 62.5 is the temperature in Fahrenheit, and 43.8% is the moisture content. If this information is sent as plain text, anyone can intercept and read it. Now, let’s use AES encryption with a secret key of “ILoveSouthDakota”. The same data is transformed into “mLgLoX5qKbn5gceFW6Lvxg==”, a scrambled message unreadable to hackers. If we change the secret key to “ILoveNorthDakota”, the encrypted result becomes “VXnOeQNi+smlozBaBNhW8g==”, which is completely different. This shows that the correct key is essential to unlock and read the original data. Note: This example is created using the online AES encryption tool courtesy of Devglan. Data Encryption Examples Below are a few examples of data encryption in agriculture: Encryption of images Various types of cameras, such as RGB, thermal infrared, depth, multispectral, and hyperspectral, are now widely used in precision agriculture for monitoring crops and livestock. These images can show detailed information about farm conditions, which producers may want to keep private. Encrypting the images helps protect this sensitive data from unauthorized access. Figure 2 shows a comparison of two crop images before and after being encrypted using AES. The encrypted version is completely unreadable. Even if hackers can intercept the image online or steal it from a memory card, they will not be able to understand it without the correct key. Four images. Two on the left show a live view of crop fields. Two on the right are scrambled due to AES encryption. Figure 2. Images of crops before (left) and after AES encryption (right). (Courtesy: Alahe et al., 2025)

<<LINE BREAKS CONTINUE>>

Encryption of GPS locations

GPS data plays a **key role** in guiding farm **equipment** like self-driving tractors and drones. It is **important** to encrypt the data to keep it **safe from hackers** or tampering (also known as spoofing). For example, many farms use differential or RTK GPS base stations that send highly accurate location signals to a machine like a planter in the field. These **signals** are often encrypted so that no one can **manipulate them**. This helps ensure the equipment stays on the right path.

Securing cloud-stored farm records

Farm management software often stores **large amounts** of sensitive **information** online, such as crop yields, field maps, financial records, and inventory. To protect this data from unauthorized access, cloud service providers often encrypt the data before saving it. This ensures that even if someone breaks into the cloud system, the saved data remains unreadable without the correct decryption keys. Some examples of farm management software that use encryption include Farmbrite, PickApp, and CropTracker.

That outweighs---it's most suffering in the US.

Asp '22 [Karen Asp; Vegan Journalist; 04-27-2022; "Is Smart Farming Making Life Worse for Farmed Animals?"; Sentient Media; https://sentientmedia.org/is-smart-farming-really-smart-for-farmed-animals/; accessed 10-19-2025] leon

As its name may imply, **smart farming** is the use of technology in **animal agriculture**, and it's something that's been around since the Industrial Revolution. The biggest difference between then and now, though? "Motorized devices are being replaced with artificial intelligence (AI)," says Ben Williamson, U.S. executive director of Compassion in World Farming, an organization aiming to end factory farming by 2040.

As a result, concentrated animal feeding operations (**CAFOs**), which is where Sentience Institute estimates that roughly **99 percent** of U.S. farmed animals live, can **automate** more easily, using **technology** like smart robotic feeders and robotic milkers for dairy cows. Data about the environment inside factory farms and the animals themselves can also be collected **more readily**. For instance, sensors linked to computers could indicate if the equipment is malfunctioning, and smart wearable tags and trackers on the animals (think of them as Fitbits for farmed animals) could reveal potential health issues and spot early signs of illness. And while VR headsets are undoubtedly too costly to provide for every farmed animal, they're another way technology is changing the way we farm animals.

<<TEXT CONDENSED NONE OMITTED>>

The above examples only touch the surface of how technology is being used in the animal agriculture industry, but no matter the mode, the goal is the same. "Smart farming is designed to increase the yields and productivity from farmed animals," Williamson says. And there's proof it's working. For instance, a farmer in Turkey was quoted in the Newsweek article as saying that prior to using VR headsets with his cows, he was getting 22 liters of milk per day. Yet after two of his cows used VR headsets, which he says gave them an emotional boost and lowered their stress because they were watching green pastures, their average milk production rose to 27 liters. And in an article posted by the European Commission, the author points to one study which found that when cows were outfitted with smart ear tags and feeders, milk yield increased by one percent and milk quality by 20 percent. Where animal welfare fits into the smart farming equation Companies producing smart farming technology do mention improved animal welfare as one benefit. But Dawkins argues that whether smart farming improves or damages animal welfare will depend on three factors. "Three developments will be crucial to the ethical evaluation of smart farming in its treatment of animals: the definition of 'welfare' it adopts, computer recognition of welfare, and crucially, whether the welfare of farmed animals is actually improved by the application of smart farming technology," she writes. There are, of course, many ways animal welfare has been defined, but no matter the definition, it's akin to how you would define human welfare. "It essentially comes down to the animals' happiness and level of suffering," says Jacy Reese Anthis, social scientist, co-founder of the Sentience Institute and author of The End of Animal Farming. "Animals want to live unconfined, be in good health, and have healthy social relationships, none of which animal agriculture allows." Even a step toward better health, something that smart farming promotes, comes with an ulterior motive, namely profits. "If you have sick animals, that's fewer animals you'll be able to sell," says Williamson, adding that Compassion in World Farming engages with the world's leading food companies to adopt meaningful animal welfare policies while tracking progress against those commitments to ensure compliance. "So animal welfare is a consideration with smart farming, but not in the same way you or I might consider it to be a plus, as the incentive to keep animals alive and healthy revolves around economics, and I think sometimes the purpose of keeping animals alive and healthy enough is just to have more of them to use."

<<LINE BREAKS CONTINUE>>

Ultimately, **smart farming** could wind up intensifying **animal suffering**. "Because you don't need as many **humans** involved with smart farming, you can increase the **number of animals** in CAFOs, which means animals will be confined in even **tighter spaces**," says Anthis, adding that more animals also means greater **disease breakouts**, which can lead to health issues for humans. "Any small gains you make in decreasing their suffering will be **outweighed** by **these increases**."

The US outweighs.

Roberson '22 [Claire Roberson; Communications Manager for Animal Equity; 09-19-2022; "Can Slaughter Truly Be Humane?"; Animal Equity; https://animalequality.org/blog/can-slaughter-be-humane/; accessed 10-26-2025] leon

But **cows**, **pigs**, and **chickens** are among the **most abused** animals. In the United States alone, approximately 427 animals, including fish, are killed every second in slaughterhouses – over **13 billion** every year. And their death is anything but 'humane.'

Farmed Animals Experience Fear In Their Final Moments

Inside the **slaughterhouse**, animals are forced **into pens**. They have just endured a **long journey** on a cramped transport truck without food or water. While they wait in the pens, the pigs can hear the screams of those being slaughtered. They tremble as they wait for their turn and look for a way to escape. And when it's their turn, they fight back, resist leaving the pen or try to run.

Workers Abuse Animals Moments Before Slaughter

A number of Animal Equality investigations have also exposed intentional **animal abuse** in these final **moments** of the animals' lives. Animal Equality released the most extensive investigation inside Mexican slaughterhouses after filming in 34 facilities. Investigators found workers beating and kicking animals and shocking them with electrical devices. Pigs, cows, and sheep were often killed while **fully conscious**.

Animal suffering is more severe.

Dawkins '17 [Richard Dawkins; British ethologist, evolutionary biologist, and author, an emeritus fellow of New College, Oxford, and was the University of Oxford's Professor for Public Understanding of Science, 09-02-2017; "Richard Dawkins: No Civilized Person Accepts Slavery So Why Do We Accept Animal Cruelty?"; transcribed from https://www.youtube.com/watch?v=_4SnBCPzBl0&; accessed 08-18-2025] leon

There's absolutely no reason as far as I can see why a **nonhuman animal**, a dog or a chimpanzee or a cow, should be any **less capable** of **feeling pain** than we can, when you think about what pain is actually doing. Pain feels like something primitive, feels like something like seeing color or smelling a rose or something like that. It doesn't feel like the kind of thing for which you need intellect. And actually you can go even further than that. You might say since pain is there to **warn** the animal **not to do that** again, an animal which is a **slow learner**, and animal which is not particularly intelligent might actually need **more intense pain** in order to **deter** it from **doing that again** than a human who is intelligent enough to learn quickly not to do that again. It's even possible that nonhuman animals are capable of feeling more intense pain than we are. I'm not sure how far I want to push that argument, but I think at least I can say there's absolutely no reason to suppose that they feel less pain than we do and we should give them the **benefit of the doubt**.

Reform is impossible.

FW '22 [Food and Water Watch; Non-Governmental Organization Group Dedicated to Solving Climate Change; September 2022; "Lab Meat Won't End Factory Farms — But Could Entrench Them"; Food and Water Watch; https://www.foodandwaterwatch.org/wp-content/uploads/2022/10/RPT2_2209_LabMeatUPD-WEB.pdf ; accessed 09-04-2025] leon

Consumers would first need to accept these novel products. They must appeal to people who enjoy meat and be comparable in taste and cost.28 This is a tall order. Scaling up **cultured meat** requires **expensive** facilities and equipment and sterile environments — such as those used in the biopharmaceutical industry.29 Moreover, consumers are **increasingly interested** in not just sustainability but nutrition; they are seeking fresh, minimally **processed foods** with short ingredient lists.30 **Cultured** and **plant-based** meats are **neither**.

Second, even if these new meat alternatives gain widespread **acceptance**, there is **no guarantee** that it will replace consumption of **farmed meat**, which is deeply embedded in **Western culture**. One study found that even if **price** and **taste** were equal, most consumers would still **choose** a beef burger over a **cultured** or **plant**-based one. This might help

explain why fast food sales of plant-based alternatives are flatlining and chains are dialing back their offerings; as the novelty wears off, customers are choosing the **familiar**.31 Meanwhile, U.S. per capita meat consumption reached an all-time high in 2020.32 Plant-based meat seems to be complementing — not replacing — meat in people's diets.

Finally, **factory farms** are baked into the U.S. **food system** through various federal **policies** and **economic incentives**.33 This dooms any market-based solution from the very start. For instance, U.S. meat production already **outstrips** domestic demand, and **surpluses are exported**. So even if everyone in the United States switched to meat alternatives, Big Ag would continue to **produce meat**. Likewise, reducing or eliminating meat consumption will **not affect incentives** to stick with the current ecologically depleting **farming systems** that prop up factory farms, such as the overproduction of **commodity crops** on monocultures.34 Both cultured and plant-based meat rely on many of the same commodities used in livestock feed and may further entrench these systems.35

Wild animals have positive value to life.

Browning & Veit '23 [Heather Browning, researcher in animal sentience and welfare at the London School of Economics; Walter Veit, Lecturer (Assistant Professor) in Philosophy at the University of Reading; 03-12-2023; PubMed Central; Positive Wild Animal Welfare; https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10008771/; DOA: 2-20-2024; //ArchanSen]

For those who argue that suffering prevails in nature, they may accept all that we have presented above and still hold that most animals will have net-negative lives. This is because the majority of animals born are of so-called 'r-selected' species, a fact that forms the basis of the primary argument presented by those in favour of the view we are opposing in this paper (e.g. Horta 2010, 2015). Johannsen (2020b) explicitly lays out the central argument (p. 12):

Premise 1: A life that's filled with suffering and ends shortly after birth is not a flourishing one, and it may not be worth living.

Premise 2: Most r-strategists live lives that are filled with suffering and end shortly after birth.

Premise 3: Most sentient individuals born into the world are r-strategists.

Conclusion: Most sentient individuals born into the world do not live flourishing lives, and their lives may not be worth living.

In this section we will challenge this argument on two grounds. Firstly, we deny that this strategy does necessarily result in a large amount of suffering (denying premise 2), and secondly, by showing that even where it is the case, it is insufficient to outweigh the positive welfare in the lives of other surviving animals.

R-selection is a life-history strategy in which animals produce a very large number of offspring, with low parental investment, where most will die quickly but a few will make it through to the next generation. This is particularly common in smaller species, such as invertebrates, as well as fish, amphibians and reptiles. In contrast there are K-selected species, like humans, that produce a small number of offspring with high parental investment in each, to ensure a high rate of survival. While these strategies are part of a larger spectrum, most animals can be described as tending toward one end or the other. These strategies ensure that most animals born will be more toward the r-selected end, as a single parent can produce hundreds or in some cases even millions of offspring, with the expectation that only a few will survive. While a large proportion of these may not even survive to birth/hatching, it still leaves a large number that will be born and will die shortly after. This is taken to mean that most animals that ever exist will have short lives with a lot of suffering – dying quickly from predation, or starvation when competing for resources against their siblings and conspecifics. Their lives are taken to be almost entirely suffering, and thus the number of animals with net-negative lives will outweigh those surviving members who have positive lives (Horta 2010).

Related to this is the economic model created by Ng (1995), purporting to demonstrate that suffering must dominate in nature, based on evolutionary and ecological factors, particularly the fact of excess production of offspring. He takes it as given that animals that

do not survive through to mating will most likely have negative welfare, though rather than providing any particular evidence for this claim, simply reflects that "it is difficult to imagine a positive welfare for such a life" (Ng 1995 p. 271). As we will discuss, even if this is true for the individuals, this does not necessarily mean that their negative experiences outweigh overall the positive experiences of their surviving relatives. Yet, many animal ethicists cited it as scientific 'proof' that animals in the wild will suffer and that we would require radical interventions. After all, Ng himself claimed that "if we can reduce the number of such miserable individuals, other things being equal; we can increase the level of over-all welfare" (p. 271). But as our previous sections demonstrated, such intuitions may well not be well-motivated.

Importantly, Ng's model relies on the 'Buddhist premise', that proposes that under a set of assumptions about the costs of enjoyment and suffering, there will be an excess of suffering over enjoyment. This he takes to imply that the pleasures associated with successful action will be less than the suffering associated with unsuccessful action. This premise was revised in a later paper (Groff and Ng 2019), showing the original model to contain mathematical errors undermining his Buddhist premise. The authors admitted that the balance between positive and negative experiences may instead go either way, depending on the living conditions of the animal. The original model "when fixed, negates the original conclusion. Instead, the model offers only ambiguity as to whether suffering or enjoyment predominates in nature" (Groff and Ng 2019, p. 39). In particular, we need to better understand the production function of pleasure and suffering. Without further understanding of the costs and benefits of affective experiences within the contexts of each different organism, it is not possible to theoretically hypothesise which is likely to dominate. However, despite this reversal, much of the damage has been done, with the original model still being cited in favour of the claim of the predominance of wild animal suffering, with the revised model still being largely ignored.

The primary reason to doubt that this reproductive strategy creates overwhelming suffering is that the lives of those that die early may not be entirely filled with suffering. Horta (2010) claims that these animals will have "little (or no) happiness in their lives" (p. 81), but as we have discussed in the previous section, there are a **wide range** of potential positive experiences available to wild animals. In the short period of their lives, they may therefore also experience small pleasures of **exploring**, **finding food** etc., and not only dizzying fear, pain and hunger. Pleasure and suffering are not directly correlated with survival and reproduction, but with the different experiences associated with these (e.g. finding food, avoiding predation, avoiding disease and injury, finding social companions). It therefore does not follow that an individual who does not survive or reproduce will not have opportunities to experience pleasure – for instance, a young animal may have **many** instances of **satiety**, **comfort**, **social bonding** etc. Additionally, though Horta (2010) takes it to be the case that death by starvation or predation will be painful enough to outweigh any sources of pleasure, we have given reasons in Sect. 2 to doubt this. Individuals at very early life-stages taken by predators are likely to die **quickly**, without prolonged **suffering**. For animals with very short lives, this may not hold, but then neither will they have lives with very many experiences so even if all experiences are characterised by suffering, they will **not amount to much in the overall total**.

It is also possible that juvenile r-selected animals have **reduced sentience** (i.e. that their conscious experience is dim, and the high of their highs and low of their lows correspondingly reduced). It is unclear exactly at which stage of development sentience emerges, and this is likely to be different for different species – ranging from pre-hatching to **several months after birth** (Mellor 2019). Where larval forms have underdeveloped neural anatomy and sense organs, it is less likely that they will have the full capacity of an adult member of their species. Without a better understanding of the neurophysiology of sentience, this possibility remains open.

There is also the possibility that there is not an **adaptive advantage** for younger animals to develop full sentience. A complex brain is costly, and is only worthwhile if it provides sufficient benefit. If it is the case that large numbers of offspring will die early, and in cases where this will be through no fault of their own (i.e. there is mostly an amount of randomness as to which animals will perish and which will survive, rather than being a result of the decisions made and actions taken by the animals themselves) then there is less advantage for animals to develop the capacity to suffer at this stage. As pointed out by Groff & Ng (2019), there is the possibility that as the number of doomed offspring increases, the suffering of each decreases, as the costs of producing suffering would be unlikely to benefit the organisms in these circumstances. Again, this is speculative and would require further research into the adaptive function of sentience, however is a potential way in which the **net suffering** of juvenile

r-selected animals may be **lower** than often claimed. Until this is better understood, it cannot be taken as strong grounds for supporting the argument for net suffering in wild animals. While Horta (2015) considers this possibility, he takes it that the overwhelming numbers of such individuals would still lead to net suffering. However, we think that with the additional considerations of less painful deaths and more positive life experiences than is often allowed, there is less reason to be confident in this conclusion.

Antitrust

1AC---Antitrust

Advantage [x] is ANTITRUST.

Monopolization will cause market crash in years.

Acemoglu '25 [Daron Acemoglu; PhD, Turkish American Economist and Professor at MIT; 02-08-2025; "The real threat to American prosperity"; Financial Times; https://www.ft.com/content/4e3f1731-3d63-4b31-88ce-c3f5157d8170; access at https://archive.ph/WRDhC; accessed 10-28-2025] leon

Others saw the "**government-tech complex**" that emerged in Trump's second term as the real culprit. With all AI and cryptocurrency regulations lifted and the Trump Department of Justice declaring that it would not apply any antitrust pressure, the tech industry **consolidated** further and a few mega-corporations came to dominate the entire sector. This not only slowed down new useful **innovations**, but laid the seeds of the big **tech crash** of 2030, when trillions of dollars were **wiped** off the economy as it became clear that most of the huge investment in AI wasn't paying off.

<<TEXT CODNENSED NONE OMITTED>>

Another school of thought contended that the rot had begun with the 46th president, Joe Biden, under whose watch inflation surged, the federal debt jumped up and regulations became more politicised and stifling for businesses — something that, despite his promises, Trump never reversed. Instead, the newly created Department of Government Efficiency (Doge), run by Trump's ally Elon Musk, focused on firing and intimidating civil servants sympathetic to the previous administration. This didn't do much to improve the business environment or competitiveness, but further weakened oversight of corruption. A basic pillar of the American century was the country's ability to shape the world order in a way that was advantageous for its own economy, including for its financial and tech industries. But the US withdrawal from the Paris Accords and the World Health Organization and the onerous tariffs imposed on allies, followed by infighting within Nato, prompted more and more countries to move away from the dollar and US financial system as their anchor. None of these explanations were sufficient to account for the sudden, unexpected decline, however. The most significant was the crumbling of American institutions. This happened both because of structural problems that long predated Biden and Trump, and also, importantly, because the actions of both presidents crushed belief in these institutions. American economic success in the era after the second world war depended on innovation, which in turn relied on strong institutions that encouraged people to invest in new technologies, trusting that their inventiveness would be rewarded. This meant a court system that functioned, so that the fruits of their investments could not be taken away from them by expropriation, corruption or chicanery; a financial system that would enable them to scale up their new technologies; and a competitive environment to ensure that incumbents or rivals couldn't block their superior offerings. These kinds of institutions matter under all circumstances, but they are especially critical for economies that rely heavily on innovation. Stability requires that people trust institutions, and institutions become more likely to fail when people think they are failing. This is what explained the sudden meltdown of US economic dynamism. Cracks were never absent in US institutions, which for most of their history had disenfranchised and discriminated against Black Americans and at times, such as during the turn of the 20th century, were captured by the wealthy and by large corporations. All the same, many citizens in the 1950s and 1960s believed in the American dream and American democracy. Democracy's bargain everywhere, and especially in the US, was to provide shared prosperity (economic growth out of which most people benefited), high-quality public services (such as roads, education, healthcare) and voice (so that people could feel they were participating in their own government). From around 1980 onwards, all three parts of this bargain started to fall away. Economic growth in the US was rapid for most of the post-1980 era, but about half of the country didn't benefit much from this. In a pattern unparalleled in the industrialised world, Americans with less than a college degree experienced a real (inflation-adjusted) decline in their wages between 1980 and 2013, while those with postgraduate degrees experienced robust growth. It wasn't only income. Postgraduates and those in specialised "knowledge" occupations increased their social standing relative to blue-collar workers and traditional office employees. Many regions of the country were gripped by long-lasting recessions as cheap imports from China and new technologies destroyed jobs, while major coastal, globally hyperconnected metropolitan centres continued to flourish. Another dimension of inequality was similarly jarring: a rapidly multiplying number of multibillionaires, not just flaunting their wealth but exercising ever greater influence over politics and people's lives. Many Americans felt that they no longer had much of a political voice. In surveys, more than 80 per cent started saying that politicians did not care about what people like them thought. They also reported incredibly low levels of trust in all branches of government, in courts, in the police and in the bureaucracy. Some of this discontent was manufactured in social media and on talk shows. But some of it was real, as on many issues politicians did not accommodate the views of large numbers of voters. For example, for a long time neither Democrats nor Republicans engaged with intensifying concerns that some voters had with illegal immigration, creating an environment ripe for demagogues and extremists to grab the spotlight. But perhaps the most important determinant of this dwindling trust in institutions was that the US had become much more polarised, making it increasingly difficult to satisfy the majority of the voters. The flames of grievance were powerfully fanned by social media, which deepened polarisation. This then further reduced trust in democracy and in public institutions. Worse, with intensifying distrust, something essential to democracy — compromise — became more and more challenging. By the 2010s something unprecedented was happening. Ever since data on this had been collected, an overwhelming majority of Americans saw democracy as the "only game in town" and gave it strong support relative to alternatives such as monarchy, military dictatorship or rule by unelected experts. That began changing, especially among young people, who reported growing scepticism about democracy and much more lukewarm support for these institutions. The cracks were visible long before Trump was first elected in November 2016. He was in many ways a symptom of those troubled times. Voters can be gullible. But their willingness to support outsiders, often with very little preparation or qualification for national office, correlates with deep discontent with the existing state of affairs and a belief that the system needs to be shaken up. One fundamental problem was that political operatives and business elites opposed to Trump never understood him in this way. In this environment, Trump quickly transitioned from being a symptom to being a cause, repeatedly breaking with democratic norms and refusing to abide by the constraints that laws and precedents set on presidential behaviour. Joe Biden was elected as president in November 2020 in part to restore stability to US institutions and strengthen democracy. He boasted that in its first 100 days, his administration "acted to restore the people's faith in our democracy to deliver". But polarisation took its toll on Biden's presidency. Democratic party activists interpreted the 2020 election results as a mandate to adopt a radical agenda of social change throughout US society, some of it starting in federal or local governments and some of it emanating from universities and non-governmental organisations, though empowered by the knowledge that the party in government favoured this agenda. Biden was arguably too weak or too beholden to the various parts of his coalition to chart a different course. For many, much of this felt like top-down social engineering, and was one of the factors that brought Trump back to power in 2025. He was once again a symptom of the times, elected despite being recognised by many as volatile, polarising and a convicted felon. Trump's second term therefore turned out to be more damaging to US institutions than his first, not just because he had been radicalised himself and came to power more prepared. It was also because the times were different. Turning points are useful to locate because they are symbolic of deeper causes of social change. In hindsight, an obvious turning point came just before Trump's second inauguration. Biden, who had four years ago made defence of democracy a main agenda item, pre-emptively pardoned his family and a number of politicians and public servants, including former Republican Congresswoman Liz Cheney and the former medical adviser to the president, Anthony Fauci. The optics were clear and ugly: Biden and his camp by this point had so little trust in US institutions that they thought only such pre-emptive pardons could stop Trump's retribution (and making the reality worse than the optics, it was only the enemies of Trump who were close to Biden that counted). Symbols matter, especially when it comes to institutions. Once it becomes accepted that institutions are not functioning and cannot be trusted, their slide intensifies and people are further discouraged from defending them. We could see this dynamic already in the late 2000s, interwoven with polarisation. Trust in institutions took a severe beating after the financial crisis of 2007-09, precisely because the conceit of a well-regulated, expertly run economy came crashing down. Understandably, many Americans reacted negatively when the government rushed to rescue banks and bankers while doing little to help homeowners in bankruptcy or workers who had lost their jobs. The inequalities that had formed became much more visible, partly because the lavish lifestyles of the bankers rescued by the government became a symbol for the gulf that had opened between regular working people and the very rich. Similarly, the critical state of US institutions became much clearer after Biden's cynical pardons, sending a signal to millions that his administration's defence of democracy was a charade. The damage to democracy thus began even before Trump ascended to power the second time. From there it deteriorated following a bewildering series of executive orders and initiatives, mostly aimed at weakening democratic institutions (for example, appointing unqualified loyalists to key posts and freeing violent participants of the January 6 Capitol attack) and firing non-loyal personnel from the civil service. While Trump's domestic agenda intensified the loss of trust in US institutions and expertise in government, his relations with foreign allies did the same for the so-called rules-based order. Of course, there was some truth to critics' contention that these rules were designed for America's benefit and that when they didn't serve it well, they were bent or broken by US politicians, diplomats and companies. But the world was not ready for Trump's tariffs, threats and military expansionist rhetoric towards Panama, Greenland and even Canada. This set the scene for a series of catastrophic governmental failures. With morale gone and key personnel fired, the US state was ill-equipped to deal with emergencies. When new pandemics arrived, the response was haphazard, and unpreparedness cost tens of thousands of lives. The few remaining independent media sources uncovered a glaring and dangerous lack of oversight of critical infrastructure, including nuclear reactors and cyber security.

<<LINE BREAKS CONTINUE>>

But the real extent of the damage became clear only with the tech meltdown of 2030. Economists and historians have now shown that a lot of this was the outcome of institutional failures and growing concentration in the industry. After Trump lifted all **roadblocks** ahead of **AI acceleration** and **cryptocurrency speculation**, there was initially a boom in the tech sector. But within a few years the industry had become even more consolidated than before, and both insiders and outsiders came to realise that only companies favoured by the administration could survive.

Gargantuan incumbents began **crushing rivals**, first by using their financial might, then by luring competitors' workers and innovators (who curiously stopped producing valuable patents once they had joined these mega-firms) and ultimately by stealing their intellectual property. By this point, US courts had lost most of their objectivity, and because the mega-firms were the administration's friends and allies, they **benefited** from favourable rulings even when they were blatantly stealing from smaller competitors and engaging in predatory pricing and vertical foreclosure to drive them out of the market.

By late 2029, many commentators were questioning what was going on in the tech industry, which had invested **heavily** in AI but had little to show for this in terms of **innovation** or **productivity growth**. There was huge enthusiasm and investment in cryptoassets, which were one by one revealed to be scams costing regular Americans billions of dollars. The AI empire had no clothes by this point, because the competitive energy had been sucked out of it. It took a while longer for the market to realise that, but when it did, a massive **stock market crash** followed.

Ephemeral messaging is the root cause---it makes enforcement impossible.

Rainer et. al **24** [Carlos, Eliot Turner, Darryl Anderson, Geraldine W. Young, Partners at Norton Rose Fullbright, "Antitrust enforcers flag Slack, encrypted email and other ephemeral messaging apps and warn of potential obstruction of justice charges and fines for a company's failure to preserve such

communications during litigation or government investigations," https://www.nortonrosefulbright.com/en-us/knowledge/publications/193cd517/antitrust-enforcers-flag-slack-encrypted-email-and-other-ephemeral-messaging-apps, 2024] etkin

On Friday, January 26, 2024, federal antitrust enforcers issued joint press releases warning of potential obstruction of justice charges and fines for a company's failure to preserve information **during** the pendency of **litigation** and government investigations, specifically calling out collaboration tools such as Microsoft Teams, Signal, Slack and other ephemeral messaging applications utilized on online communication platforms or similar technologies that allow, permit or even facilitate the **immediate** and irretrievable **destruction** of communications and documents.

The Department of Justice (DOJ) Antitrust Division and the Federal Trade Commission (FTC) announced that each agency was updating language contained in the agencies' standard preservation letters and specifications for all second requests, voluntary access letters and compulsory legal process, including grand jury subpoenas, to address the use of collaboration tools and ephemeral messaging platforms, which updates the agencies stated were necessary to reinforce longstanding obligations requiring companies to preserve materials during the pendency of government investigations and litigation, particularly in light of these new methods of collaboration and information sharing tools.

The agencies observed that while documents created through use of online messaging platforms and related technologies have fallen squarely within the agencies' prior document requests, companies have **not always** properly **retained** these types of **documents** during government investigations and litigation. Collaboration tools and instant messaging apps such as Microsoft Teams, Signal and Slack were identified specifically as ephemeral messaging technologies that enable the immediate and **irretrievable** destruction and **electronic purge** of communications and documents. Deputy Assistant Attorney General (AAG) Manish Kumar of the Antitrust Division remarked that the agencies "expect that opposing counsel will preserve and produce any and all responsive documents, including data from ephemeral messaging applications designed to hide evidence," warning that any failure to do so "…may result in obstruction of justice charges." Deputy AAG Kumar noted further that "[t]hese updates to our legal process will ensure that neither opposing counsel nor their clients can feign ignorance when their clients or companies choose to conduct business through ephemeral messages." Where opposing counsel and companies fail to preserve and produce information contained in ephemeral messaging applications, the FTC warned that it may pursue civil spoliation fines in civil litigation and may refer the conduct for criminal prosecution through the FTC's Bureau of Competition's Criminal Liaison Unit.

Employee communications—through both official and unofficial channels—are **routinely targeted** by federal enforcement agencies in **litigation** and **investigations**. As technology continues to improve and evolve, new methods of collaboration and information sharing tools will continue to be created, adopted and used by companies and their employees, including tools that allow for company communications and documents to evaporate or disappear instantaneously via ephemeral messaging capabilities. The manner and methods in which companies permit, monitor, preserve and archive these types of communications are becoming increasingly more important to government enforcement agencies as evidenced by the DOJ's inclusion of specific guidance earlier last year for assessing how companies govern employees' use of personal devices, communication platforms and messaging applications. On March 3, 2023, the DOJ released an update to its Evaluation of Corporate Compliance Programs guidance (ECCP Guidance), which serves as guidance for prosecutors when evaluating a corporate compliance program.2 The updated ECCP Guidance includes new guidance for assessing how companies govern employees' use of personal devices, communication platforms and messaging applications. The newly updated ECCP Guidance explains how the DOJ, going forward, will consider when evaluating corporate compliance programs and investigating potential misconduct, a company's specific policies and procedures related to the use of personal devices, online communications platforms and messaging applications, including ephemeral messaging applications. Under the newly updated ECCP Guidance, the DOJ now will consider the following:

Whether and how policies relating to personal devices and communications platforms are "tailored to the [company's] risk profile and specific business needs";

Whether and how the policies (and other mechanisms) ensure that business-related data and communications are "accessible and amendable to preservation," including specific inquiry into "[w]hat preservation or deletion settings are available to each employee" and also "the rationale for the company's approach to determining which communication channels and settings are permitted";

Whether and how the company's policies with respect to same have been communicated to employees; and

Whether and how the company has enforced its policies on a regular and consistent basis, including specific inquiry into whether and to what degree messaging applications—including ephemeral messaging applications—have "**impaired** in any way the organization's

compliance program or its ability to **conduct** internal **investigations** or **respond to requests** from prosecutors or civil enforcement or regulatory agencies".

These encryption technologies are the death knell of anti-trust.

Weick and Nicolaides **24** [Daniel, Special Litigation Counsel in Attorney General's Antitrust Bureau, Jamie, Disputes Lawyer at Hausfeld, "Vanishing act: The impact of ephemeral messaging on civil antitrust conspiracy litigation," https://www.hausfeld.com/fr-fr/what-we-think/competition-bulletin/vanishing-act-the-impact-of-ephemeral-messaging-on-civil-antitrust-conspiracy-litigation, 2024] etkin

But most civil antitrust conspiracy cases do not feature such clear evidence. In those cases, plaintiffs must rely on **circumstantial evidence**. Circumstantial evidence comprises 1) proof of parallel conduct in a concentrated industry (like nearly simultaneous price increases), 2) proof of each defendant's awareness of the other firms' conduct, and 3) proof of "plus factors" making conspiracy a reasonable inference from the first two elements.[8] The relevant plus factors may include evidence that the alleged conspirators engaged in actions contrary to their unilateral interests, evidence that the alleged conspirators had a motivation to conspire, evidence regarding frequent communications between firms, and other traditional conspiracy evidence.[9] Ultimately, because consciously parallel conduct without an agreement does not violate the Sherman Act,[10] "a plaintiff seeking damages for a violation of § 1 must present evidence 'that tends to exclude the possibility' that the alleged conspirators acted independently."[11]

Increasing use of ephemeral messaging products could **obviously deprive** plaintiffs of **direct evidence** (i.e., the content of written messages), and it could also impact plaintiffs' ability to show **plus factors** involving "interfirm communications."[12] While cartelists may use telephone communications or face-to-face meetings to coordinate their activities without creating a written record, or may delete their SMS text messages to avoid production of the message contents, phone carrier records, hotel receipts, documentation of trade association conferences, and other evidence can at least show the fact that the alleged conspirators had the opportunity to and did communicate, as well as the frequency of those communications. Likewise, while employees can delete their emails, businesses can act to retain emails created on their servers, and other forensic evidence may still show that the deletion of email communications occurred. But as the Google Play Store litigation illustrates, ephemeral messaging applications—especially those using encryption technology—can **automatically delete** such messages so that **no record** of the communications **remains** at all.

These technologies will create **substantial opportunities** for cartel participants to engage in the communications necessary to **coordinate** their **conspiracies** without creating any record of having communicated. Not only would auto-deletion deprive plaintiffs of the content of the communications, but it will deprive them of the ability to prove that the communications occurred in the first place. Ephemeral messaging apps could therefore limit the ability of civil plaintiffs to collect **crucial** early **evidence** of interfirm communications and thus prevent them from even targeting the right individuals for discovery in **build**ing their **cases**.

Missing evidence of party communications also could deprive civil litigants of the important benefits of government enforcement actions, where government agencies can use subpoena power to thoroughly develop the evidentiary record before they proceed with a civil complaint or criminal charge.[13] The DOJ has historically insisted on criminal prosecution of price-fixing agreements, meaning that cases where the evidence does not rise to the level of proof **beyond a reasonable doubt** typically fall to private litigants **without public enforcement**. While certain civil matters like the Apple/e-books conspiracy (where the hub-and-spoke theory and the new technology made the applicability of the per se rule against price-fixing debatable)[14] or the recent litigation over alleged price-fixing on generic pharmaceuticals (where the size and importance of the impacted commerce drew suits from the vast majority of U.S. state attorneys general)[15] may involve government enforcers, agencies following current policy will likely focus on price-fixing matters with the sort of direct evidence that could support a criminal conviction. If ephemeral messaging apps make it **impossible** for the DOJ to prove beyond a reasonable doubt that price-fixing occurred, then there may be no governmental enforcement for private litigants to rely on in developing their cases.

The AFF bans ephemeral messaging---other countries prove.

James Andrew **Lewis** et. al **17**, PhD from University of Chicago, Senior Fellow at CSIS, “The Effect of Encryption on Lawful Access to Communications and Data,” CSIS, 2/8/17, https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data, tristan + leon

Third, communications content is **increasingly ephemeral**. Some chat and e-mail applications are moving to adopt transient messaging by **automatically deleting** messages from devices and servers immediately after they are viewed (e.g., Snapchat and Wickr). Ephemeral messaging platforms and data retention policies that favor minimization render data **inaccessible** to law enforcement, regardless of encryption. If the data, even if it is not encrypted, is **deleted**, it **cannot be provided** to law enforcement. Importantly, this affects both metadata and the content of communications.

<<TEXT CONDENSED NONE OMITTED>>

Fourth, companies are taking steps to offer products with the above features on widely used consumer messaging platforms and are enabling these features by default. This significant trend means that users no longer have to manually turn on encryption. In other words, billions of users worldwide have adopted unrecoverable encryption without even knowing it as mobile messaging companies have incorporated features into their products and services that guard against eavesdropping or intercepting communications, but also prevent the companies themselves from being technically capable of accessing user data. END-TO-END ENCRYPTED MOBILE MESSAGING Mobile messaging applications such as WhatsApp, Facebook Messenger, Message, Telegram, Skype, Line, and others are rapidly becoming the dominant mode of communication around the world. Growing demand for instant messaging (IM) means that its share of global message traffic is estimated to grow from 50 percent to 63 percent in the next few years. Instant messaging traffic is expected to grow more than 20 percent annually through 2019, nearly doubling to almost 100 trillion messages per year (or almost 274 billion per day).4 Many of these apps, called over-the-top (OTT) services and applications, have recently moved to adopt end-to-end encryption, making them inaccessible to law enforcement agencies. Three of the world’s top twelve mobile messaging apps, as measured by monthly active users (MAUs), have enabled unrecoverable end-to-end encryption by default. This means more than 1.5 billion individuals globally use end-to-end encrypted messaging applications. Many of the largest messaging platforms have adopted end-to-end encryption (E2EE) in the last year, including WhatsApp, Facebook Messenger (not by default), and Viber. The largest end-to-end encrypted messaging app by number of users is WhatsApp, which implemented E2EE by default in April 2016.5 Less than 10 percent of Internet users in the United States use WhatsApp, but for many other countries WhatsApp is a primary mode of communication. Approximately 34 percent of global Internet users have WhatsApp on their phones. In Latin America and the Middle East about 66 percent of Internet users use WhatsApp.6 Juniper Research estimates that roughly 108 trillion messages were sent 2016.7 Almost 90 percent of those messages are instant messages and e-mails, the majority of which are encrypted, often using HTTPS encryption that is accessible to law enforcement through the service provider. Based on the share of messaging platforms that employ end-to-end encryption, we estimate that about 18 percent of total communications traffic uses end-to-end encryption and is inaccessible to law enforcement. The share of unrecoverable encryption as a share of total communications traffic is likely to grow, as instant messaging becomes increasingly dominant. Meanwhile, growth in e-mail and short message service (SMS) messaging, which are usually accessible to law enforcement agencies, is expected to be flat. The rapid growth of IM means that its share of global message traffic will increase from 50 percent to 63 percent.8 These estimates imply that even if the share of instant messages that are end-toend encrypted remained constant, more than 22 percent of global messaging will be end-to-end encrypted and inaccessible to law enforcement by 2019 as instant messaging becomes an increasingly dominant mode of communication. Some messaging applications present challenges for law enforcement that are unrelated to encryption. For example, Kik is a messaging platform that is known to be used by child predators, who use it to identify victims and share sexually explicit material. Kik is not end-to-end encrypted, but it does not retain most user data on its servers, making it impossible to service search warrants.9 Telegram, a popular messaging app, supports end-to-end encryption but does not enable it by default. However, law enforcement has struggled to access even unencrypted communications over Telegram, which hosts its data in Switzerland. Telegram is popular with terrorist groups and was used by the jihadi killers of a French priest in August 2016.10 Developed by Russian Internet entrepreneurs who were forced out of Russia and fled to Germany, Telegram refuses to comply with law enforcement requests for data.11 FULL DISK ENCRYPTION The use of unrecoverable encryption is a growing trend in the mobile space, particularly as full-disk encryption (FDE) is becoming the norm for a growing share of consumer devices. Apple is the largest provider of mobile FDE in the world. Approximately 13 percent of all mobile devices globally run iOS, and more than 95 percent of all iOS devices currently run iOS 8 or higher, which Apple says even they cannot access.12 Device encryption on Apple phones is a likely a bigger challenge for U.S. law enforcement than for other countries because 44 percent of all mobile devices in the United States run iOS. Google’s Android is the largest mobile operating system in the world, making up more than 86 percent of the global mobile market. Currently, less than 10 percent of Android devices have enabled FDE, partly because the Android mobile industry is not vertically integrated. Although the operating system is developed by a single company (Google), there is a relatively large number of device makers, which means that the Android ecosystem is less coordinated than Apple’s system.13 Android is also more popular in countries like China and India where the average consumer is more price sensitive and thus more likely to purchase less powerful mobile devices that do not have enough processing power to support FDE without compromising user experience. Because about 47 percent of all mobile devices in the United States have FDE (the global average is 21 percent), FDE on mobile devices likely poses a larger problem for U.S. law enforcement than it does for other countries. This could change dramatically if all iOS and Android devices adopt FDE as their default, resulting in the majority of data stored on smartphones becoming inaccessible to law enforcement in all countries.14 E-MAIL ENCRYPTION In contrast to mobile messaging apps, end-to-end encrypted e-mail is not widely used by consumers or enterprises and is unlikely to be widely adopted, largely for business reasons. E-mail users have different expectations than instant messaging users. They expect to be able to access stored e-mails, recover account passwords if they forget them, access their e-mail from any device, and send e-mails to their friends using different e-mail platforms. End-to-end encryption renders all of these functions difficult or impossible. Moreover, most e-mail services are free, and providers monetize the service by mining user data, including the content of e-mails. None of the major consumer e-mail providers have deployed end-to-end encryption. The largest e-mail providers globally, with hundreds of millions of users, have adopted secure socket layer (SSL)/transport layer security (TLS) encryption, but none of them use end-to-end encryption that is unrecoverable by law enforcement. By comparison, end-to-end encrypted e-mail providers such as ProtonMail and Tutanota are tiny, with just 1 million users each.15 But growth of end-to-end encrypted e-mail is rising dramatically in the aftermath of recent large-scale e-mail hacks, such as the intrusions into the Democratic National Committee and Yahoo.16 Data on Going Dark The data that is available on the effect of encryption on law enforcement is limited. Senior law enforcement officials have referred to incidents where encryption presented a challenge, but have not provided a comprehensive picture.1 There is some information, however, on cases where law enforcement has attempted to access data, such as through Title III wiretaps and device seizures, and were thwarted by unrecoverable encryption. This may not represent the full scope of the challenges faced by law enforcement, but it presents a starting point for understanding the effect of encryption use. ENCRYPTION AND TITLE III WIRETAPS Data on the effect of encryption on Title III wiretaps suggests that encryption has not significantly hampered law enforcement investigations. Title III wiretaps are used for real-time surveillance of communications in motion. To execute a wiretap, investigators must demonstrate probable cause to obtain a warrant and seek assistance from service providers covered by the Communications Assistance for Law Enforcement Act (CALEA2 to execute the intercept. According to annual Title III wiretap reports compiled by the U.S. Court System, a very small share of Title III wiretaps encounter encryption, and the majority of those are ultimately decrypted. The first time that unrecoverable encryption was reported in a Title III wiretap was in 2012. That year, 67 wiretaps encountered encryption, of which four were unrecoverable. From 2012–2015, 152 Title III wiretaps encountered encryption, of which 30 were unrecoverable. During this period more than 14,500 wiretaps were ordered, meaning that just 0.2 percent of wiretaps encountered unrecoverable encryption.3 Law enforcement officials argue that this statistic is misleading. Title III wiretap applications are complex and time consuming. Investigators know what apps are unrecoverable, so they often do not even bother to request wiretaps in cases where such apps are being used by suspects. Instead, they pursue other investigative techniques to get the evidence needed for prosecution. ENCRYPTED MOBILE DEVICES SEIZED BY LAW ENFORCEMENT Comprehensive statistics on encryption as an obstacle to law enforcement are currently unavailable, but based on available data, full disk encryption on mobile devices poses a greater challenge. In April 2016, Amy Hess, executive assistant director of the FBI’s Science and Technology Branch, testified that about 30 percent of the more than 3,000 mobile phones that the FBI seized in the previous six months were password protected, and in about 13 percent of those cases the FBI was unable to access any data on those phones, which is about 120 phones.4 She also said that she expects that number to continue to grow as unrecoverable encryption is deployed on more devices. State and local law enforcement are also affected. For example, the Los Angeles Police Department and Los Angeles County Sheriff had a total of 650 inaccessible phones in evidence as of the end of February 2016, while the New York County District Attorney’s office seized 423 inaccessible phones between October 2014 and October 2016.5 The 423 inaccessible phones seized by the New York County District Attorney’s office represent approximately 34 percent of the total phones seized by that office over the same period, and relate to a range of cases including murders, sex crimes, and complex financial crimes.6 USE OF UNRECOVERABLE ENCRYPTION BY MALICIOUS ACTORS Islamic extremists are using unrecoverable encryption to attempt to evade law enforcement and intelligence agencies, with ISIS providing instructions for their followers on how to use encryption in recruiting and coordinating operations. Abdelhamid Abaaoud, the European ISIS leader who directed the terrorist attacks on Paris in November 2015, included computer security in his training for his operatives, teaching them to use open source TrueCrypt disk encryption software to hide data on their computers from law enforcement.7 Al Qaeda’s media arm even produced its own encrypted communications app, Amn al-Mujahid, to allow its members to communicate.8 However, most terrorists do not appear to rely on encryption for their operational communications. They evade surveillance using a number of alternative means. The Paris attackers, for example, used burner phones9 and other means (such as couriers or prearranged code words) to evade surveillance. Terrorist groups use encryption, but we found no evidence that this is their primary means of securing their communications, because they either avoid the use of Western communications technology or use communications techniques to evade surveillance that do not rely on encryption. We examined publicly available material on six major terrorist attacks—Mumbai, London, Boston, San Bernardino, Paris, and Brussels—plus several failed attempts (New York and Koln) and data taken from devices recovered in the conflicts in the Middle East. In no instance did we find evidence that encryption played a determinative role in these incidents. The attackers relied on surprise and responder confusion to achieve success.10 While online recruitment by terrorist groups is a major concern, encryption also does not appear to play a major role in this. In some instances (e.g., London, Brussels), propinquity better explains recruitment—the attackers all lived in the same neighborhoods and had similar social backgrounds. In other cases, terrorists used a combination of false identities and multiple website and chatroom addresses to attempt to evade surveillance. When a site is forced to move, informal networks based on chatrooms or e-mail inform potential recruits of the new network address. This word-of-mouth system to distribute new addresses is very effective. The ability to use social networks for recruitment does not rely on encryption. CRIMINAL USE To get an accurate sense of how unrecoverable encryption affects security and public safety, we need to look at the net effect. Being able to obscure data and communication has both positive and negative results. The benefits accrue in cybersecurity and privacy. The costs accrue in decreased surveillance capabilities, affecting law enforcement and counterterrorism. Communications surveillance and lawful access to communications are invaluable tools in deterring and prosecuting crime and in counterterrorism. What is not clear is how much the current use of unrecoverable encryption actually degrades these capabilities and whether there is any concomitant increase in criminal activity. Child pornography, which was almost eradicated in the 1980s, has rebounded because the Internet made it easier to engage in this behavior, increasing an incredible 15 times (by the number of cases) between 1995 and 2006.11 This increase occurred well before the advent of widely available unrecoverable encryption. The principal cause of the increase is access to the Internet making this easier to share. The effect of encryption, however, complicates efforts to identify and prosecute those who engage in child pornography. Drug traffickers have used encryption to evade surveillance for years. The Zeta organization of Mexico even built its own mobile, encrypted, communications network a decade ago.12 Encrypted apps provide a cheap alternative to proprietary networks. Drug traffickers used encrypted messaging app Surespot to evade law enforcement as early as 2014.13 Guadalajara cartel boss Rafael Caro Quintero used WhatsApp video messages to communicate with other cartel leaders,14 while Sinaloa cartel boss Joaquin “Chapo” Guzman attempted to use a Blackberry to secure his messages while in hiding. The use of encryption changes the nature and complexity of antidrug operations, but as one political official put it: “Drug dealers are using encrypted devices, money launderers are using encrypted devices but they are still being caught, we are still making arrests.”15 There are many troubling examples, but judging from the available data, the number of cases affected by encryption is small, ranging from a few dozen to several hundred, varying from jurisdiction to jurisdiction. What the FBI and other law enforcement agencies are worried about is a potential future where large technology companies will provide unrecoverable encryption by default for a growing share of communications platforms. The use of encryption is a subset of a larger problem created by the Internet. In addition to its immensely positive contributions to societies, the Internet also makes it easier to engage in illicit behavior, a trend exacerbated by both the transborder nature of Internet activities and the absence of enforceable legal constraints on online behavior. Malicious actors’ use of encryption is an outgrowth of this larger problem, not its cause. For now, the most likely effect of greater use of unrecoverable encryption is to make prosecution of criminals more onerous. It likely does not mean an increase in the number of people engaging in the criminal activity. Alternative sources of digital evidence are available, such as metadata or unencrypted video, audio, and other types of data increasingly available with the expansion of the so-called Internet of Things. But the rules and policy around leveraging these new data sources are unclear and law enforcement lacks the technical expertise for collection and analysis of this data. SURVEILLANCE AND ENCRYPTION In many ways, the debate is about surveillance. Societies need to weigh the risk that encryption restrictions could pose to privacy (and, perhaps, to sales in the global market) against the potential risks to public safety and security from decreased surveillance. Alternate investigative techniques using metadata and advanced data analytics could compensate, to a degree, for greater encryption use by allowing agencies to identify potential terrorists or criminals. This alternative is cumbersome and unsatisfactory in many ways, but our assessment is that while greater use of encryption makes digital surveillance less efficient, it does not render it ineffective. Since precise metrics on risk and effect do not exist for encryption, we are often left with conflicting opinions. Those who must manage the risk of crime or terrorism fear the rate of increase in unrecoverable encryption use creates unacceptable risk; those who fear surveillance argue that any restriction on encryption is the real source of risk. Better policymaking requires better data, including monitoring the rate of change in the number of investigations and prosecutions thwarted by encryption and the role of encryption in terrorist operations. Global Concern, but No Global Consensus

<<LINE BREAKS CONTINUE>>

One shortcoming of the U.S. encryption debate is its overwhelmingly American focus. Encryption is not just an American issue. **Several** other countries favor **limits** on the use of **unrecoverable encryption** and have moved to **block** its use. Sometimes this involves laws and regulations, while other times it involves secret agreements between governments and companies. In other cases, there are **legal requirements** that service providers design and operate their systems in a way that allows them to **decrypt** data for the government.

More than **half** of the world’s Internet users live in countries with laws that allow them to **mandate** some sort of **decryption** assistance from companies or individual users. Most people live in countries where encryption use is restricted in some way, although how these restrictions are enforced varies widely. To assess global attitudes toward encryption, we looked at 15 countries that account for more than 60 percent of global Internet users. Of these 15 countries, 7 (who are home to roughly half of the world’s internet users) have laws that allow them to require encryption providers to maintain the capability to decrypt data. The other 8 countries are smaller, accounting for about 16.6 percent of global Internet users, and many of these countries, while not requiring recoverability, use other policies to manage encryption.

Monopolies crush growth---antitrust is key.

Jordan ‘25 [Jilayne Jordan; Graphics and Communications Specialist at Camoin Associates; 09-03-2025; "6 Reasons Monopolies Are Bad for Consumers and the Economy"; Camoin Associates; https://camoinassociates.com/resources/6-reasons-monopolies-are-bad-for-the-economy/; accessed 10-28-2025] leon

A **monopoly** is formed when one company controls the **entire market** for a particular product or service. This company becomes the only option for consumers, and without competition, it can charge any price it wants, reduce quality, and/or limit choices without fear of losing customers. The **primary motivations** for forming monopolies are **profit** and **power**.

<<TEXT CONDENSED NONE OMITTED>>

Monopolies can be created using both mergers and acquisitions. A merger occurs when two separate companies merge to form a single entity. One example of this is when Kraft Foods and The H.J. Heinz Company merged to become The Kraft Heinz Company in 2015. Not all mergers

create monopolies, but those that do (usually referred to as horizontal mergers) occur when businesses that directly compete with each other decide to join forces. An acquisition occurs when one business buys another, the buyer absorbs the purchased company's assets, and the purchased company then ceases to exist. Acquisitions can be friendly or hostile. Hostile acquisitions (or "takeovers") happen when a company buys a majority of the target company's stock shares or makes an offer to shareholders without the approval of the company's executives. Examples of acquisitions include InBev's hostile takeover of Anheuser-Busch in 2008 and AT&T's friendlier acquisition of Time Warner in 2018. Why Are Monopolies Bad for Consumers and Our Economy? Monopolies disrupt the balance of a competitive market, which harms consumers and our country's economy in six ways: 1. Higher Prices

<<LINE BREAKS CONTINUE>>

Without competition, monopolies can **set prices** as high as they want knowing their customers have no other options.

2. Lower Quality and Reduced Efficiency

Competition pushes companies to improve products, offer quality customer service, and operate efficiently. Without it, there's **little incentive** to do anything **better** or differently.

3. Fewer Choices

If one company controls an entire market, you're stuck with their product or service whether you like it or not.

4. Barriers to Entry

When one company controls an entire market, it's nearly **impossible** for new businesses to **compete** and survive. This lack of competition slows innovation and economic growth. In a competitive market, companies strive to outdo each other, which often benefits customers and consumers.

5. Unfair Power Dynamics Affecting Other Areas of the Economy

Monopolies can wield **too much influence** over suppliers, distributors, customers, and even governments. This power imbalance can lead to policies and practices that benefit the **monopoly** at the expense of others.

6. Job Losses

When companies are merged or acquired to form a monopoly, the **consolidation** typically has direct local and regional economic impacts, including closing stores/facilities/factories and **laying off** workers.

<<TEXT CONDENSED NONE OMITTED>>

How Does the US Government Regulate Monopolies? Antitrust Laws The federal government regulates monopolies through antitrust laws aimed at preventing anti-competitive behavior, promoting market competition, and ensuring consumer welfare. They include: The Sherman Act (1890) is the cornerstone antitrust law in the US. It prohibits any contract, combination, conspiracy, or monopoly that restrains trade or commerce. This includes banning anti-competitive agreements and price fixing. The Clayton Act (1914) supplements the Sherman Act by addressing more specific anti-competitive practices, such as price discrimination, exclusive dealing arrangements, and mergers that reduce competition. In addition, most states have their own antitrust laws, which are enforced by state attorneys general or private plaintiffs. In the case of the Kroger-Albertsons merger in my community, both the federal government and the State of Washington filed separate antitrust lawsuits against the company that were tried at roughly the same time in different courts. Enforcement Agencies and Processes

<<LINE BREAKS CONTINUE>>

The Federal Trade Commission (FTC) and the Department of Justice (DOJ) are tasked with enforcing our country's **antitrust laws** and addressing instances of **unfair competition** and deceptive business practices.

These two enforcement agencies tend to focus on different industries or markets and consult with each other before opening new investigations to avoid duplication of effort.

Premerger notification filings, correspondence from consumers or businesses, Congressional inquiries, or news reports about consumer or economic subjects can trigger a federal antitrust investigation by either agency.

If the investigation reveals that antitrust laws have been violated, the agencies may attempt to negotiate with the company to rectify the situation through a consent agreement. If the company is unwilling to do that, the federal government may **initiate** formal **legal proceedings** similar to a federal court trial but before an administrative law judge. Like a typical court case, **evidence** is

presented by the **plaintiff** (the government agency) and the defendant, testimony is given, and witnesses are examined and cross-examined.

If the judge determines antitrust laws have been violated, a **cease-and-desist** order may be **issued** or the judge may ask the **agencies** and the company to submit **potential remedies** and then determine what steps will be taken. The company can then appeal the judge's decision. In successful appeals, the judge's decision may be overturned completely or the penalties reduced.

Economic decline causes global hotspot escalation.

Jiang '25 [Shuguang; Marie Claire Villeval; Zhengping Zhang; Jie Zheng; March 3; Doctorate, Professor at the Centre for Economic Research, Shandong University; PhD, Research Professor in Economics at the National Center for Scientific Research, University of Lyon; PhD, Associate Professor at Shandong Technology and Business University; PhD, Professor at the Centre for Economic Research, Shandong University; Hal Science, "War and Peace: How Economic Prospects Drive Conflictuality," p. 1-4, https://hal.science/hal-04967990/file/War_and_peace_WP3March25.pdf]

Although peace and development are central themes of our time, various forms of conflict – between nations, ethnic groups, organizations, and individuals– **remain pervasive**. High-profile **geopolitical tensions**, such as the ongoing conflicts between **Russia** and **Ukraine** and in the **Middle East**, serve as **stark reminders** of the **preciousness** of **peace**. The shifting global landscape and **power struggles** among major nations are **particularly concerning**. **Thucydides's Trap**, a concept popularized by political scientist Graham T. Allison (Allison, 2015, 2017), draws from the ancient Greek historian Thucydides, who noted that the rise of a **new power** often led to conflict with an **established** one. The idea has gained significant attention in contemporary international relations, particularly in the context of the perceived rivalry between the United States and China.

Historical accounts underscore the **recurring nature** of power transitions **leading** to **conflict**. For example, the rise and fall of British naval mastery, as discussed by Kennedy (2017), and broader analyses of war and change in world politics by Gilpin (1981) illustrate the Thucydides Trap.1 Allison (2015) refers to **16 historical cases** over the past 500 years where a rising power challenged an established power, finding that **12** resulted in war. The two World Wars are **also** prominent historical **cases**. These historical perspectives highlight the potential for instability and conflict during significant power shifts.

This deterministic view has been challenged by scholars like Lee (2019) and Chan (2020) who argue that conflict is **not inevitable** and that other factors, particularly **economic conditions**, can influence the trajectory. This argument is further supported by analyses of historical power shifts, such as Britain's response to its relative decline (Friedberg, 2021) and the dynamics of power transitions in Asia (Shambaugh, 2005).2 This opens the door to investigating whether economic conditions can alter the course toward **conflict** or **coop**eration in power dynamics.

Economic conditions are undeniably **crucial** in **determining** international **conflicts**. **World War II**, for example, was significantly influenced by the Great **Depression**. Economic prospects also influence domestic politics and conflicts. Collier and Hoeffler (2004) suggest that economic conditions largely **determine** the opportunity for **rebellion** in **civil conflicts**, while Blattman and Miguel (2010) and Ray and Esteban (2017) identify lower income levels and weak economic growth as **strong predictors** of **civil wars**. Gartzke (2007) and Mitra and Ray (2014) highlight the role of economic development in reducing war and mitigating communal violence. The role of economic factors in power transitions is more complex. Gilpin (1981) and Kennedy (2017) argue that disparities in economic growth can disrupt the balance of power, potentially leading to instability and conflict.

Building on this, we explore how economic prospects affect the likelihood of cooperation and conflict between rising and established powers. We hypothesize that **growth prospects** encourage **coop**erative strategies, as both parties stand to benefit from mutual gains. Economic **interdependence** driven by **positive economic prospects** can foster **stronger trade** relations, **investment**, and **collaboration** in technology and infrastructure, creating a **stabilizing effect** where **both powers** have a **vested interest** in maintaining **peace**. **Conversely**, **bleak** economic prospects can **intensify competition** over **limited resources**. An established power may perceive the rising power's growth as a

threat to its dominance, prompting **preemptive actions**. Similarly, a rising power facing **economic difficulties** may adopt **aggressive strategies** to **secure resources** and **markets**, **escalating tensions**.

<<TEXT CONDENSED NONE OMITTED>>

Better understanding the interactions between the dynamics of power and economic trajectories provides valuable insights into the potential for cooperation or conflict on the global stage.3 However, numerous confounding factors make it difficult to isolate the causal effect of economic prospects on the natural occurrence of conflicts. It is also impractical to create real conflict scenarios in the real world to test these hypotheses. Therefore, we used a laboratory experiment to simulate interactions between two entities undergoing a power shift under varying economic prospects. While this experiment cannot capture the full complexity of international or commercial relations, it does allow us to study the causal relationship between economic prospects and conflict in a power-dynamic context under controlled conditions. To achieve this, we designed a dynamic power rivalry game where two players in fixed pairs, A and B, simultaneously decide how to allocate a pie in each period by either choosing to "Maintain Status Quo" or "Challenge". If both maintain the status quo, the pie is shared equally. If one or both challenge, the pie size shrinks by a social loss coefficient, and the remaining pie is distributed according to the players' relative strength, which shifts over time. Player A represents the rising power, starting with low relative strength, which increases each period. Player B, the established power, starts with high relative strength, which declines over time. Across the 21 periods of the game, their strengths undergo a symmetrical reversal, with Player A starting at 0.2 and Player B at 0.8, each shifting by 0.03 per period. Players incur a cost when choosing to challenge. We compared three economic prospect conditions across between-subjects treatments, independent from the players' actions: in the Constant treatment, the pie size remains constant across periods at 20,000 tokens; in the Decline treatment, the pie size starts at 30,000 tokens and decreases by 1,000 tokens per period; and in the Growth treatment, the pie starts at 10,000 tokens and increases by 1,000 tokens per period. The Nash equilibrium of the game predicts that Player B will challenge in the first eight periods, while Player A will challenge in the last eight, with both players maintaining the status quo in the remaining periods. Notably, the different economic prospects do not alter this equilibrium. In contrast, our results show that the proportion of challenges from both players, as well as the overall conflict incidence rate, is highest in the Decline treatment and lowest in the Growth treatment. The differences between these treatments are significant across various metrics. Only the Growth treatment reaches a conflict rate significantly lower than the Nash equilibrium. Specifically, Player A (the rising power) challenges significantly more than the equilibrium in both the Decline and Constant treatments but challenges insignificantly less than the equilibrium in the Growth treatment. Player B (the established power) challenges less than the equilibrium in all treatments but only significantly so in the Growth treatment. Further analyses of the behavior of different types of players with absolute advantage, characterized notably as "money maximizers" who always challenge or "peace lovers" who never challenge, support the robust pattern that growth prospects reduce conflict. We also show that the initial action is crucial in determining subsequent behaviors. Though triggering a conflict is socially inefficient, growth prospects help enhance social welfare. Exploring the mechanisms driving the different impacts of decline and growth prospects, we reject potential explanations in terms of differences in wealth accumulation. A behavioral model with psychological costs for challenging and reciprocity helps rationalize why different economic prospects lead to divergent routes in terms of conflict and cooperation when relative powers shift. This model shows that an established power is less likely to challenge when expecting its rival's reciprocity. Given its expectations of the rival's psychological costs, an established power is less likely to initiate a challenge in the Growth treatment than in the other treatments.

<<LINE BREAKS CONTINUE>>

To test the real-world relevance of the dynamics observed in our experiment, we conducted a preregistered online survey experiment in the United States with a representative sample of 813 individuals. After presenting each of two scenarios describing long-term global economic prospects –one optimistic and the other pessimistic –, respondents reported their beliefs about the probability that **tensions** between China and the **U**nited **S**tates would **escalate** into conflict over the next decade. In line with our **lab**oratory **experiment** findings, respondents perceived a **significantly higher** likelihood of conflict in the **slow-down scenario** than in the growth scenario. Moreover, most respondents believed that major powers are **most likely** to engage in conflict when global economic prospects are **declining** and **least likely** under global economic **prosperity** and growth trends.

Extinction!

Clare '23 [Stephen Clare; Effective Altruism Writer; June 2023; "Great power war"; 80000 Hours; https://80000hours.org/problem-profiles/great-power-conflict/; accessed 12-05-2024] leon

A modern **great power war** could see **nuclear weapons**, bioweapons, autonomous weapons, and other destructive **new technologies** deployed on an unprecedented scale.

It would probably be the most destructive event in history, shattering our world. It could even threaten us with **extinction**.

<<TEXT CONDENSED NONE OMITTED>>

We've come perilously close to just this kind of catastrophe before. On October 27, 1962 — near the peak of the Cuban Missile Crisis — an American U-2 reconnaissance plane set out on a routine mission to the Arctic to collect data on Soviet nuclear tests. But, while flying near the North Pole, with the stars obscured by the northern lights, the pilot made a navigation error and strayed into Soviet airspace.1 Soviet commanders sent fighter jets to intercept the American plane. The jets were picked up by American radar operators and nuclear-armed F-102 fighters took off to protect the U-2. Fortunately, the reconnaissance pilot realised his error with enough time to correct course before the Soviet and American fighters met. But the intrusion enraged Soviet Premier Nikita Khrushchev, who was already on high alert amidst the crisis in Cuba. "What is this, a provocation?" Khrushchev wrote to US President John F. Kennedy. "One of your planes violates our frontier during this anxious time when everything has been put into combat readiness." If the U-2's path had strayed further west, or the Soviet fighters had been fast enough to intercept it, this incident could have played out quite differently. Both the United States and the USSR had thousands of nuclear missiles ready to fire. Instead of a nearly-forgotten anecdote, the U-2 incident could have been a trigger for war, like the assassination of Franz Ferdinand. Competition among the world's most powerful countries shapes our world today. And whether it's through future incidents like the lost U-2, or something else entirely, it's plausible that it could escalate and lead to a major, devastating war. Is there anything you can do to help avoid such a terrible outcome? It is, of course, difficult to imagine how any one individual can hope to influence such world-historical events. Even the most powerful world leaders often fail to predict the global consequences of their decisions. But I think the likelihood and severity of great power war makes this among the most pressing problems of our time — and that some solutions could be impactful enough that working on them may be one of the highest-impact things to do with your career. By taking action, I think we can create a future where the threat of great power war is a distant memory rather than an ever-present danger. Summary Economic growth and technological progress have bolstered the arsenals of the world's most powerful countries. That means the next war between them could be far worse than World War II, the deadliest conflict humanity has yet experienced.

<<LINE BREAKS CONTINUE>>

Could such a war actually occur? We can't rule out the possibility. **Technical accidents** or diplomatic **misunderstandings** could spark a conflict that **quickly escalates**. Or international tension could cause **leaders** to **decide** they're better off **fighting** than **negotiating**.

<<TEXT CONDENSED NONE OMITTED>>

It seems hard to make progress on this problem. It's also less neglected than some of the problems that we think are most pressing. There are certain issues, like making nuclear weapons or military artificial intelligence systems safer, which seem promising — although it may be more impactful to work on reducing risks from AI, bioweapons or nuclear weapons directly. You might also be able to reduce the chances of misunderstandings and miscalculations by developing expertise in one of the most important bilateral relationships (such as that between the United States and China). Finally, by making conflict less likely, reducing competitive pressures on the development of dangerous technology, and improving international cooperation, you might be helping to reduce other risks, like the chance of future pandemics. Our overall view Recommended Working on this issue seems to be among the best ways of improving the long-term future we know of, but all else equal, we think it's less pressing than our highest priority areas (primarily because it seems less neglected and harder to solve). Scale There's a significant chance that a new great power war occurs this century. Although the world's most powerful countries haven't fought directly since World War II, war has been a constant throughout human history. There have been numerous close calls, and several issues could cause diplomatic disputes in the years to come. These considerations, along with forecasts and statistical models, lead me to think there's about a one-in-three chance that a new great power war breaks out in roughly the next 30 years. Few wars cause more than a million casualties and the next great power war would probably be smaller than that. However, there's some chance it could escalate massively. Today the great powers have much larger economies, more powerful weapons, and bigger military budgets than they did in the past. An all-out war could kill far more people than even World War II, the worst war we've yet experienced. Could it become an existentially threatening war — one that could cause human extinction or significantly damage the prospects of the long-term future? It's very difficult to say. But my best current guess is that the chance of an existential catastrophe due to war in the next century is somewhere between 0.05% and 2%. Neglectedness War is a lot less neglected than some of our other top problems. There are thousands of people in governments, think tanks, and universities already working on this problem. But some solutions or approaches remain neglected. One particularly promising approach is to develop expertise at the intersection of international conflict and another of our top problems. Experts who understand both geopolitical dynamics and risks from advanced artificial intelligence, for example, are sorely needed. Solvability Reducing the risk of great power war seems very difficult. But there are specific technical problems that can be solved to make weapons systems safer or less likely to trigger catastrophic outcomes. And in the best case, working on this problem can have a leverage effect, making the development of several dangerous technologies safer by improving international cooperation and making them less likely to be deployed in war. At the end of this profile, I suggest five issues which I'd be particularly excited to see people work on. These are: Developing expertise in the riskiest bilateral relationships Learning how to manage international crises quickly and effectively and ensuring the systems to do so

<<LINE BREAKS CONTINUE>>

By any measure, such a war would be by far the most **destructive**, dangerous event in human history, with the potential to cause **billions of deaths**.

The probability that it would, on its own, lead to **humanity**'s **extinction** or unrecoverable collapse, is contested. But there seems to be some possibility — whether through a famine caused by **nuclear winter**, or by reducing humanity's **resilience** enough that something else, like a **catastrophic pandemic**, would be far more likely to reach extinction-levels (read more in our problem profile on nuclear war).

General

1AC---Narrative---Lay

Adaptation is an imperative.

Ann Louise **Wagner 20**, Representative for Missouri's second congressional district, "Lawful Access to Encrypted Data Act," xx/xx/20, https://tinyurl.com/ycyr9pyh, tristan

Encryption technology is an important tool for safeguarding data and promoting cybersecurity. However, bad actors **exploit** "warrant-proof" forms of **encryption** to shield dangerous and illegal activities from legitimate **law enforcement investigation**. These crimes include human **trafficking**, **child sexual abuse**, **drug trafficking**, **terrorism**, and numerous others. Increasingly, service providers and device manufacturers are **refusing** to **cooperate** with law enforcement in accessing encrypted evidence, even when issued a **warrant** supported by **probable cause**. Without this assistance, investigations into some of the **most serious crimes** affecting our communities around the country are substantially frustrated, delayed, or even prevented **entirely**. This puts our communities and our **national security** at risk.

Coronavirus lockdowns have substantially heightened risks for children who are targeted online for sexual exploitation. Victims of exploitation and their families have pleaded with service providers, device manufacturers, and other technology companies to take responsible steps to make sure their platforms are not abused by bad actors. But many of these companies continue to prioritize **profits** and the absolute privacy of abusers **over** the safety, security, and privacy of children. This market failure allows **criminals** to operate with **impunity** and must be corrected through legislative action.

During a Senate Judiciary Committee hearing in 2019, Manhattan District Attorney Cyrus Vance argued that as the technology industry evolves, the law **must evolve with it**. This has been the case **throughout** American history. When private sector harms that cannot—or **will not**—be addressed by **industry** are identified, Congress **must act** to preserve public safety. In the communications industry, Congress passed the Communications Assistance for Law Enforcement Act to preserve wiretapping capability; in the financial services industry, Congress required banks to adopt systems to detect money laundering and provide data to law enforcement; in the pharmaceutical industry, Congress passed laws requiring manufacturers to go through an FDA process to ensure drugs were safe; in the agriculture industry, Congress passed the Pesticide Control Amendment of 1954 establishing safety limits; and in the construction industry, Congress passed the Clean Air Act of 1970 to protect Americans from asbestos exposure. This is government's role when an industry cannot police itself and is exposing Americans to danger. Similarly, as the technology industry evolves, the **Lawful Access** to **Encrypted Data** Act would ensure law enforcement can still properly **investigate** and **prosecute** criminal activity while **maintaining** the privacy rights of Americans.

Alternatives can't solve.

Erik J. **Dahl 20**, Professor at the Naval Postgraduate School, Pre-doctoral fellow at the Belfer Center at Harvard's Kennedy School of Government, PhD from Tufts University, BA from Harvard University, "The Key to Lawful Access: An Analysis of the Alternatives Offered in the Encryption Debate," Defense Technical Information Center, 8/1/20, https://apps.dtic.mil/sti/html/trecms/AD1126508/, tristan

The literature on the encryption debate often asserts that the government should seek other options for obtaining the information it needs instead of mandating lawful access. Lawful hacking is one such option, when law enforcement and intelligence agencies exploit vulnerabilities to defeat encryption and access data in a readable format. Literature on the subject argues that lawful hacking is an adequate balance between the two sides of the encryption debate. However, when analyzed in the context of case studies of counterterrorism and criminal investigation, it **falls short** because of its **unreliability** in accessing data and its **infeasibility** in **implementing** the method across U.S. police agencies.

Other alternatives also **fall short**. Metadata, or data about data, also fails to replace lawful access adequately since it does **not reveal** the important **content** of **communications**, specifically, valuable evidence in criminal **investigations** and actionable **intelligence** in counterterrorism pursuits. Compelling users to disclose

passcodes of devices permitting access is **unusable** in instances where users are not **present** to unlock a device. In addition, the courts have not settled on the implications for **civil rights**. Accessing backup data in the cloud is also **inadequate** as it is **easily avoided** by nefarious actors and must often be affirmatively engaged to back up devices fully. While all these alternatives are in use today by law enforcement, they do **not** meet the needs of public safety and homeland security agencies, even if viewed in unison.

AND current backdoors prevent effective surveillance while actively abandoning company safety. Lawful access is a legitimate front door that flips privacy, security, inevitable crackdown incentives, & backdoor creation.

Corn '17 [Geoffrey S. Corn; George R. Killam Jr. Chair of Criminal Law; Director, Center for Military Law & Policy Texas Tech University School of Law. Professor Corn served in the U.S. Army for 21 years, retiring in the rank of Lieutenant Colonel. He served as the Army's senior law of war expert advisor, tactical intelligence officer in Panama; supervisory defense counsel for the Western United States; Chief of International Law for US Army Europe; Professor of International and National Security Law at the US Army Judge Advocate General's School; and Chief Prosecutor for the 101st Airborne Division; Encryption, Asymmetric Warfare, and the Need for Lawful Access, 12-1-2017; William & Mary Bill of Rights Journal, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4905083; accessed, 10-21-2025] Aaron

*E2EE = end to end encryption

I. FOURTH AMENDMENT **REASONABLENESS** AND THE BALANCE OF INTERESTS

Assessing the legality of government efforts to surveil "dark" spaces, whether motivated by law enforcement or counterterrorism interests, must begin with the Fourth Amendment. In one of my previously published articles, which has since evolved into a chapter for the book, The Cambridge Handbook of Surveillance Law, I argue that **the Fourth Amendment imposes no barrier to enactment of laws requiring feasible government access to encrypted data**.26 The focus of that chapter evolved from
the substantial public debates surrounding the San Bernardino iPhone "incident."27 Many critics of the government, including the aforementioned chapter's co-author, questioned the wisdom and legality of government efforts to demand access codes to the E2EE embedded in the iPhone used by the deceased terrorist in that incident.28

For me, this issue raised the important question of whether the government has the authority to, and ought to, require encryption designers and manufacturers to preserve the means to enable government agents to **lawful**ly access private data stored on the devices they market. While many **critics** of such a proposal lamented the idea of government mandated "backdoor" access to private data,29 I viewed this as a requirement to build into the encryption an actual front door.30

In my view, **backdoor access** connotes **clandestine** or surreptitious **access**.31 This, I argued, is exactly what the government will be compelled to pursue and **exploit** when access through a proverbial **front door is impossible** because there is no **front door**.32 However, by creating a highly **secure front** door, it is possible to achieve a **mutually satisfactory, balanced alternative:**

To be clear, this "split key" proposal is not a subterfuge method of creating backdoor access to data. Unlike a backdoor, which generally refers to an undisclosed vulnerability in an application or device, a front door is a **well-documented** and **clear** mechanism for both **encrypting and decrypting** data, whether it be data in motion (communications) or at rest (stored data). To be secure, encryption should be subject to **rigorous testing**. Thus, its presence should be open to the public and available for attack, both in laboratories and in the real world. This is the only real way to evaluate the trustworthiness of encryption, with vulnerabilities being corrected as they are discovered, to strengthen the protocol and its implementation constantly. Essentially, a front door is the digital equivalent of a big, ingeniously engineered lock on the only entrance to an otherwise secure building. It is a lock that has been **tested** by every available

lock picker and found to be secure, with any identified weaknesses being **constantly fixed**. Such a lock is always **superior** to a **secret** entrance in the rear of a building.33

Such front door access would better serve the interests of both privacy and security, as each would be effectively balanced.34 First, by "**splitting**" the encryption key and **entrusting** part of it to a **neutral organization** devoted to **privacy protection**, the individual will be provided enhanced protection by imposing a greater burden on the government to access the key.35 Second, by requiring compliance with normal **Fourth Amendment justifications** and **authorizations to engage in surveillance and seizure of any data, the data will be protected with no less vigilance than the protection of the home**.36

Of course, creating a front door will inevitably facilitate government access to private data **when properly and lawfully authorized**. This reality is contrary to the objectives of many privacy advocates.37 Some even argue that such a creation is, in effect, a subterfuge backdoor:

These opponents frame efforts to preserve such access as a call for the creation of "backdoors" that can be exploited by the U.S. and any other government. They argue that the creation of backdoors will introduce unacceptable vulnerabilities in products and systems and point to examples where, in the past, such vulnerability have been exploited by hackers.

As I have argued previously, such a suggestion is shortsighted, as it is this approach that actually further enables exploitation by hackers. 39 **When front door access is eliminated** from E2EE (or any other type of data storage), a determination that access to that data is **necessary** and lawful will compel **gov**ernment agents to work to **identify**, if not **create, backdoor** acces**s**.40 In such situations, there are strong incentives for that access to be **clandestine**, because disclosing the access point will in turn **alert** the manufacturer to a vulnerability requiring a security patch.41 It would be unwise for the government to reveal the backdoor, only to then disclose it.42 As a result, an **actual privacy vulnerability**, subject to **exploitation** by non-government actors, may persist.43

Furthermore, it is likely that the government may identify such "backdoor" vulnerabilities even when not engaged in surveillance efforts directed against specific targets as part of overall data protection operations. Without confidence that data access could be facilitated through **lawful** front door access, the government would have a **powerful incentive** not to share this information with the manufacturer or service **providers**. In short, **front door access** incentivizes government cooperation with the private sector to **identify** and **prevent backdoor breaches**, which ultimately **enhances protection** of private data from **unlawful** or unauthorized access.44

Reasonable people will inevitably differ on the proper balance between privacy and public security implicated by encryption technology, as well as how encryption facilitates exploitation of "dark spaces" by dangerous and nefarious actors. However, it is legitimate that a **balance between these interests should be the goal of law and policy makers**. Those who argue that no government effort to ensure lawful access to these dark spaces can be tolerated without sacrificing essential liberty are comfortable with technological creation of impenetrable zones of privacy. While such zones will obviously maximize the protection of privacy from government intrusion, they will do so at a cost. As I argued in my prior chapter, I believe an impenetrable zone of privacy is inconsistent with the underlying rationale of the Fourth Amendment:

Balancing the competing interests of collective societal security and individual liberty is central to the Fourth Amendment touchstone of reasonablenes**s**. The notion that the Fourth Amendment provides an individual right to an impenetrable zone of privacy is therefore inconsistent with the text and judicial interpretation of the amendment. Instead, balance remains the operative concept: protection against unreasonable search and seizure inherently acknowledged that the people can be subjected to

reasonable searches and seizures. In short, the **amendment never imposed an absolute restraint on government surveillance, even when directed against the interests protected by the amendment's text (persons, homes, papers, and effects).** Instead, the people were provided an absolute right to be secure against **unreasonable government intrusions** into those places and things protected by the Fourth Amendment.45

That key constitutional provision certainly does not mandate government action to guard against the creation of such a zone, nor does it require the government to tolerate such zones.46 Thus, from a regulatory perspective, the Fourth Amendment is probably best understood as neutral on the question of whether government should seek to mandate preservation of access to encrypted zones of privacy.47

But what the Fourth Amendment has historically tolerated—reasonable government measures to investigate and discover crime and other threats to public security— should be instructive in this debate.48 Reasonableness, after all, is as the Supreme Court reminds us, the "touchstone" of the Fourth Amendment.49 That touchstone of reasonableness, in turn, is consistently defined by balancing individual privacy with societal interests in effective law enforcement.50 With the exception of dangerous medical procedures to recover evidence from within a suspect's body,51 even the most carefully protected zone of privacy—the home—is subject to government intrusion when properly authorized.52 If the most fundamental source of protection from government intrusion into a citizen's privacy is defined by a reasonable balance between **privacy** and **security**, advancing this **balance** should be the **ultimate objective** of **lawmakers** addressing the difficult question of how to deal with "dark spaces." Requiring preservation of encryption keys to facilitate lawful government access to private data is, in my view, a rational manifestation of this balance of interests. In contrast, allowing for the continued creation and enhancement of technology that seeks to create **impenetrable** zones of privacy **distorts** this balance.

Ultimately, there are only three virtually undeniable constants in this debate.53 First, the **market** will continue to incentivize the **development** of **encryption** technology that frustrates, and ideally prevents, government access to **private communications**.54 Second, while these **innovations** will be **intended** to preserve the privacy of law abiding citizens, the **dark spaces** they create will offer exploitation opportunities for individuals and **groups** engaged in activities that **threaten society**.55 And third, **the government** will **constantly endeavor** to **access** these dark spaces, precisely because of the **risks** inherent in allowing such exploitation.56 Furthermore, the nature of national security threats, most notably terrorist threats targeting the U.S. homeland, have magnified the government's interest in penetrating these spaces.57

II. ASYMMETRY AND THE ADAPTIVE ENEMY

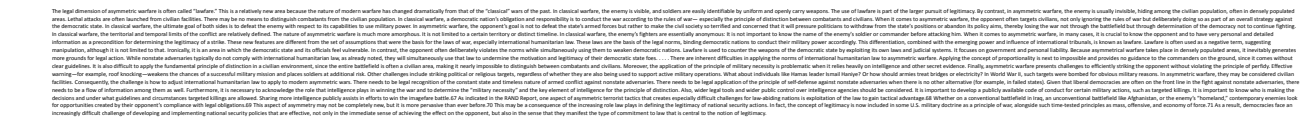
Concern over feasible access to encrypted communications is no longer simply a question of balancing privacy against the interests of effective law enforcement. Today, the risks attendant with "dark space" communications transcend criminal threats and are inextricably intertwined with counterterrorism efforts.58 This should come as no surprise. The **United States is engaged in an ongoing armed conflict against multiple transnational terrorist organizations.**59 While the notion that response to this threat qualifies as an armed conflict remains controversial for many international law experts, the fact remains that the **U.S. perceives** the nature of the threat posed by both **al-Qaeda** and **ISIS** as transcending that of ordinary criminal activity.60 Instead, the **national decision** to treat the **ongoing battle** against these **threats** as an **armed conflict** indicates a **willingness** to use **expanded means** and legal **authorities** to disrupt and disable these groups.61

Of course, these enemies do not engage in and employ analogous debates or handwritings over the appropriate legal framework for their terrorist activities. Instead, they embrace tactics that constantly seek to exploit enemy vulnerabilities in order to offset the superior material and information capabilities of their opponents—a phenomenon characterized by the term, "asymmetric warfare."62 Interestingly, there is no consensus definition of asymmetric warfare.63 However, as the following summary indicates, it generally refers to conflict between conventionally disparate enemies, with the inferior enemy seeking to offset its weakness by identifying and exploiting vulnerabilities of the conventionally superior opponent: Asymmetric warfare is generally understood to be a conflict in which the strengths and sizes of the

opponents do not mirror each other. The side with the conventional disadvantage is probably incapable of winning through direct, conventional warfare. It must seek victory through other methods that exploit weaknesses in the superior conventional power's capacity to prevail. Examples include the Maoist Peoples' War against the Imperial Japanese Army, the Vietnamese dau trahn strategy in the First and Second Indochina Wars, and al-Qaeda's tactics in the WOT [(War on Terror)].64

So characterized, there is nothing new about asymmetric tactics, which have been part of military theory and doctrine dating back to the writings of Sun Tzu.65 However, the struggle against today's transnational terrorist threats has resurrected the focus on how to effectively address asymmetric threats, threats that challenge our national security capabilities well beyond the "battlefield." 66 A Rand Report explains the characteristics and challenges associated with this modern permutation of asymmetric warfare:

<<<TEXT CONDENSED FOR READABILITY NONE OMITTED>>>



<<<LINE BREAKS CONTINUED>>>

This aspect of asymmetry intersects directly with the issue of government surveillance access to "dark spaces." **Remotely radicalized, homegrown terrorists** are assessed as among the most significant terrorist threats faced by Western nations.72 Furthermore, attacks in Paris, Brussels, and other major cities demonstrate the risk of small, well-organized attack cells operating in relative plain sight.73 Whether it is a **lone wolf**, or a small **cell** of organized **operatives**, communication is obviously **essential** for their **success**. And, because it is no mystery that the government is constantly seeking to identify and preempt terrorist attacks, it must be **self-evident** to such individuals that identification and exploitation of **dark** communication **zones** will **substantially** enhance their **likelihood of success**. Investigations into several attacks, such as the **ISIS Paris** bombings and the **Brussels** airport bombing, indicate that operatives relied on **WhatsApp** for vital **communications.** 74

The ready **availability** of **E2EE** with no built-in **front door** access will almost **certainly** be viewed by those engaged in **terrorist**ic activities as the **communication**s **method** of choice. Like all aspects of asymmetric warfare, they will seek to exploit what is viewed as a self-inflicted vulnerability to the maximum extent. The **more confident** they are in the **immunity** of their communications **from timely government surveillance**, the more likely it is they will rely on such dark spaces. But this also means that the government is all that more likely to increase efforts to **penetrate** such spaces. And this really frames the ultimate question in the encryption debate: does increasing the difficulty of lawful government access ultimately advance or compromise legitimate privacy interests? The answer to this question may be derived in part from the multipronged legal framework the U.S. relies on for counterterrorism operations.75

Other countries have moved past the US already, causing privacy erosion

Velasco 10-9 [Gwen Velasco; LLB Graduate at the City Law School, 10-9-2025, "The BluePrint Brief", No Publication, https://theblueprintbrief.com/articles/apples-encryption-fight-with-uk-reignites-over-ic/ 10-30-2025] Ewan

Commercial Impact

For Apple, the challenge is as reputational as it is legal. Disabling Advanced Data Protection for U.K. users effectively downgrades local security standards, risking customer confidence among privacy-conscious consumers and developers.

The stakes also extend beyond the U.K. U.S. lawmakers have warned that compliance with the order could conflict with the CLOUD Act, which governs cross-border data access. If Apple were to comply, it could face contradictory legal obligations under U.S. and U.K. law.

Operationally, maintaining separate encryption regimes across jurisdictions introduces technical and compliance risks. Divergent key-management systems and **data-handling rules increase the chance of system vulnerabilities**. For global tech companies, the message is clear: privacy features are no longer just product design choices, they are regulatory flashpoints.

If Apple concedes even partially, it could embolden other governments to seek similar access, leading to a patchwork of encryption standards that undermine global privacy protections.

How Legal Teams Get Involved

As Apple's appeal progresses, multiple legal and compliance functions are actively engaged:

Regulatory & Compliance Counsel

Coordinate with the Investigatory Powers Commissioner's Office (IPCO) to interpret compliance requirements while defending Apple's encryption position.

Assess potential conflicts with the Human Rights Act, GDPR, and international data-transfer rules.

Prepare reporting frameworks if encryption changes materially affect user privacy.

Product & Privacy Counsel

Collaborate with engineers to evaluate whether any design changes could introduce new legal exposure.

Conduct privacy impact assessments and ensure users are properly informed about any alterations.

Draft user communications that maintain transparency without compromising Apple's legal position.

Litigation & Risk Teams

Manage the Tribunal case and prepare for potential follow-on claims from consumers or advocacy groups.

Monitor how any ruling might set precedent for future encryption or data-access disputes.

Assess global litigation risks if the case encourages similar demands from other jurisdictions.

Government Relations & Policy Teams

Engage with U.S. and EU regulators to align approaches to lawful access and encryption.

Manage policy dialogue to preserve Apple's privacy reputation while maintaining compliance diplomacy.

Track potential reforms to the Investigatory Powers Act and anticipate long-term compliance shifts.

To protect liberty, security comes first

Etzioni 16 [Amitai Etzioni. First University Professor at GW. Former Thomas Henry Carroll Ford Foundation Professor at the Harvard Business School, Senior Advisor to the White House, Professor of Sociology at Columbia University, Chairman and founder of the International Society for the Advancement of Socioeconomics. Dr. Etzioni is the author of 19 books, and was ranked by a 1982 study as the leading expert of 30 who made "major contributions to public policy in the preceding decade."; Spring 2016; "End to End Encryption, the Wrong End"; South Carolina Law Review; https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=4179&context=sclr; DOA: 10/26/2025] doobz

D. How Liberty is Lost

The ideological case in favor of UE draws on the numerous changes made in American law and that of numerous other countries following the 9/11 terrorist attack that have been considered excessive, the Snowden revelations, the absence of major terrorist attacks on US mainland for more than a decade, and the rise of general support for libertarian and civil libertarian ideas. These are summed up by the argument that the US is sacrificing liberty to enhance safety.'1 1

A common narrative goes as follows: first, the government, in the name of national security or some other such cause, trims some rights, which raises little alarm at the time. Then a few other rights are curtailed. Soon, more rights are lost and, gradually, the whole institutional structure on which liberal democracy rests tumbles. (Statements that the US has already been turned into a police state, that Americans lost their right to privacy and free speech, and so on and on, are so overblown they need no refutation).

However, there are **very few** instances of nations that lost their liberty because of such **incremental erosion** of rights. On the contrary, the evidence shows that typically the relationship **runs the other way** around: when democratic institutions and policies do not provide an adequate response to new challenges they are **undermined**.112 There are many cases in which liberty was lost when governments did not provide basic security to their people. The **Afghans** welcomed the **Taliban** when their country was in anarchy following the retreat of the USSR.1 3 The **Russians** welcomed **Putin** when their country suffered a major crime wave; after the collapse of the USSR.1 4 The **Egyptians** welcomed **military rule** after two years of revolutionary upheaval. Many in Libya, Syria, and Iraq miss the safety of the old regimes.

Following the 9/11 attacks, when the public was most concerned about additional attacks from sleeper terrorist cells on short order, many Americans were willing to support a strong government, including one that would set aside many basic individual rights." 5 **78%** of Americans expressed willingness to "give up certain freedoms to gain security.""16

However, in the subsequent period, as the government did take numerous and varying measures to enhance public safety and no new attacks occurred, the public **gradually restored** its commitment to the rights-centered regime. As the government vigorously enacted measures to protect the public the public's support for constitutional democracy was reaffirmed. That is, when the government reacted firmly to a major challenge, support for constitutional democracy was sustained rather than undermined. In short, to protect our rights, the government needs to provide a reasonable level of security.

US adoption is key to global standard-setting.

Jim **Baker et. al 19**, Former General Counsel at the FBI, “Moving the Encryption Policy Conversation Forward,” 9/10/19, https://carnegieendowment.org/research/2019/09/moving-the-encryption-policy-conversation-forward?lang=en, tristan

Attend to International Dynamics

While this paper focuses on the United States, the **U.S. debate** is not happening in a vacuum; it will **affect** (and be affected by) choices made in **other countries** and by non-U.S. technology **companies**. (Recent papers published by the Encryption Working Group assess the environment in Australia, Brazil, China, Germany, India, and the European Union.6) **Any** proposed approach should be adaptable **beyond** a U.S. setting, both to **enhance commonality** and to **reduce** the burden of **implementation**. Policymakers should consider the viability of any proposal in light of users and devices crossing borders. They should further consider that U.S. policies will give **legitimacy** to **replication** by other nations, including those with weaker judicial protections and records on human rights. Finally, policies should be considered in light of the effect they will have on U.S. foreign policy interests.

2AC

Econ

2AC---AT: Econ

Consumers don't care that much about their privacy.

Eric **Manpearl 17**, Senior Fellow at the Robert S. Strauss Center, J.D. from the University of Texas School of Law, M.A. from Lyndon B. Johnson School of Public Affairs, "Preventing 'Going Dark': A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate," SSRN, 11/15/17, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3068578, tristan

A lawful access requirement's potential harm to the market share and economic viability of U.S. companies is the strongest argument for not mandating such a requirement. Certainly, the Snowden disclosures had a **negative impact** on U.S. companies in their immediate aftermath, but **confidence** in U.S. companies seems to have **rebounded**. In the fourth quarter of 2016, Facebook reported that it had **1.86 billion** users who logged on at least once a month.' 5 9 This is up from the **1.16 billion** users who logged on at least once a month in the second quarter of 2013, when Snowden first disclosed NSA programs. 1 6 0 In 2015, 70% of Facebook users logged on daily, which is an increase from the 63% who logged on daily in Aurst 2013, in the immediate aftermath of the Snowden disclosures.' Also, **Google** announced in February 2016 that Gmail has over **one billion** active users. 16 2 This is an **increase** from the 900 million active users Gmail had in 2015, when it became the most popular email service in the United States, and from the 425 million active users Gmail had in 2012, **prior** to the Snowden disclosures. 163 Of these Gmail users, 75% accessed their accounts on mobile devices, too." These statistics do **not** indicate that consumers are deeply **distrustful** of U.S. companies and refuse to use U.S. products and services.

Further, a recent study surveying 1510 participants, including both information technology security experts and non-experts, from the United States, United Kingdom, and Germany, found that **privacy** and **security** only play a **minor role** in people's decisions to use a particular mobile instant messenger.1 65 The **primary reason** that participants gave for using a mobile instant messenger was whether **friends** were using the messenger:1 66 46.1% of participants from the United States, 48.2% of participants from the United Kingdom, and 54.9% of participants from Germany stated this was the main reason they used a particular mobile instant messenger. 167 On the other hand, only a **small percentage** of participants stated the main reason they used a mobile instant messenger was because of privacy and security.1 68 Only 5.6% of participants from the United States, 3.4% of participants from the United Kingdom, and 13.1% of participants from Germany stated this was the main reason that they used a particular mobile instant messenger.1 69

Consumer pressure may not truly be driving the move toward more encryption; instead, companies may be pressuring each other to move in this direction. Consumers seem to care **more** about being able to be connected to **friends**, having **easy to use** and **reliable** products, and having **sleek interfaces** and useful applications, and seem **willing** to **sacrifice** some privacy and security in exchange. If consumer pressure is not driving this shift, then perhaps the fear that U.S. companies will lose market share and that the economic viability of U.S. companies would be hurt by a lawful access requirement is **overstated**. As long as U.S. companies continue to lead in the areas consumers care about the most, while still making the most secure products and services possible that comply with a lawful access requirement, U.S. companies will likely continue to dominate the technology market.

People don't think apps are secure even with encryption.

Dr. Verena **Zimmermann et. al 18**, Professor at ETH Zurich, "Finally Johnny Can Encrypt: But Does This Make Him Feel More Secure?," ACM Other conferences, 9/27/18, https://dl.acm.org/doi/abs/10.1145/3230833.3230859, tristan

End-to-end (E2E) encryption is an effective measure against privacy infringement. In 2016, it was introduced by **WhatsApp** for all users (of the latest app version) quasi overnight. However, it is unclear how non-expert users perceived this change, whether they trust WhatsApp as a provider of E2E encryption, and how their communication behavior changed. We conducted semi-structured interviews with twenty WhatsApp users to answer these questions. We found that about **half** of the participants perceived that **even with** E2E encryption, their messages could **still** be **eavesdropped**, for example by hackers and other criminals,

governmental institutions, or WhatsApp's employees and cooperation partners. Many participants correctly identified sender and recipient as weakest points after the introduction of E2E encryption, but misconceptions were still present. For instance, users thought that messages were transmitted directly between two devices without being forwarded or stored on a server, or interpreted 'end-to-end' as a temporally end of communication. The majority of users stated to **mistrust** WhatsApp and its E2E encryption and presumed image-related reasons for the cost-free implementation. While most participants did **not** change their **communication behavior**, they reported to use protection strategies such as sending sensitive content via alternative channels even after the introduction of E2E encryption.

Impacts are minimal.

Wire ’25 quantifies [Wire; Encryption Blog; 03-07-2025; "Protecting Business Communication: The Encryption Challenge & Solution"; Wire; https://wire.com/en/blog/why-most-business-communication-is-still-unencrypted; accessed 10-27-2025] leon

You may find it surprising, but according to various estimates, between **60** and **80 percent** of business **communications** (chat, voice, video, email, **document sharing**, etc.) is still **unencrypted**. In many cases, even **solutions** that provide encryption are **often vulnerable**.

Last year’s **Salt Typhoon** hack of multiple **U.S. telecommunications** companies highlighted **significant vulnerabilities** in our communication infrastructures. These intrusions **granted** attackers access to sensitive phone calls, text messages, and extensive **user metadata**, underscoring the critical need for robust security measures.

If your organization uses Teams, you may think you’re well protected, but if you take a minute to scan this blog post by secure data specialists Virtru, you’ll see that you may not be as secure as you imagined. If your team uses Slack, maybe you should read this post from the Mimecast blog about high-profile Slack data breaches over the last few years.

And if your response to these threats was to switch to consumer tools like WhatsApp and Signal, they may still expose user metadata or be susceptible to exploitation by advanced persistent threat groups.

So, why is so much business communication still unencrypted? The answer is actually pretty simple. **Most** communications platforms were **designed to be efficient** at communications, and **security** has always been a **secondary concern** - usually addressed after system design has matured. At Wire, we look at security differently. At Wire, security and usability have always gone hand in hand. The end result is a platform that delivers the security organizations require while offering the ease of use and flexibility teams need to work efficiently.

We’re in a recession.

Hawkinvest 25. 10/06/2025. Long-time stock market investor focused on strategic buying opportunities with dividend and value stocks. "The U.S. Is In Recession: 1 Million Layoffs In 2025 And LEI Data Says It All". Seeking Alpha. https://seekingalpha.com/article/4828069-the-us-is-in-recession-1-million-layoffs-in-2025-and-lei-data-says-it-all

Summary

The U.S. economy is likely **already** in a recession, masked by AI-driven capex and **delayed** official **recognition** by the NBER.

The Leading Economic Index and jobs data are flashing clear **recession** signals, with layoffs rising and hiring plans at their weakest since 2009.

Despite deteriorating economic fundamentals, the stock market remains overbought and complacent, fueled by AI optimism and expectations of Fed rate **cuts**.

Investors should not wait for an official recession call to de-risk portfolios, as historical parallels suggest significant downside risk ahead.

Democracy

2AC---AT: Democracy

Trump is tanking democracy AND nuked the ability of the US to promote democracy abroad.

Brands 25 [Hal Brands; Senior Fellow AEI studying US foreign policy; 9-28-2025; American Enterprise Institute - AEI; https://www.aei.org/op-eds/global-democracy-is-failing-will-the-us-save-it-or-kill-it/; DOA:11-16-2025] auraine

Billions of people now lived in countries that were relatively free, humane and insulated despotic cruelty and arbitrary rule. The strength and support of a **democratic superpower** were indispensable to all this **world-changing progress**, which is one reason democracy's global future feels so **precarious** right now.

The clash of ideas has always been shaped by the clash for power: From ancient times to the present, the dominant form of government has tended to follow the preferences of the era's dominant states. During the 20th century, and especially since World War II, America helped **democracy flourish** globally, by aiding its growth in distant regions and holding its most lethal foes at bay. But **for the last two decades**, democracy's influence has **slipped** as aggressive autocratic powers have **surged**. Now, democracy's global fortunes are being threatened by changes in America itself.

President Donald Trump has taken a **wrecking ball** to America's **democracy-promotion infrastructure**. Trump's antidemocratic behavior — his nearly boundless assertions of executive authority, his threats against political opponents — have made it far from unthinkable that the US might take an illiberal turn.

The global ascent of democracy was inextricable from America's rise as a liberal superpower. The forecast for free institutions will be **dire** if the US **drops out** of the intensifying struggle to shape the world's political future — **or**, much worse, if it becomes a force for **illiberalism** around the globe.

The alternative is worse---the government will just move to more invasive surveillance.

Corn 17 [Geoffrey S. Corn; George R. Killam Jr. Chair of Criminal Law; Director, Center for Military Law & Policy Texas Tech University School of Law. Professor Corn served in the U.S. Army for 21 years, retiring in the rank of Lieutenant Colonel. He served as the Army's senior law of war expert advisor, tactical intelligence officer in Panama; supervisory defense counsel for the Western United States; Chief of International Law for US Army Europe; Professor of International and National Security Law at the US Army Judge Advocate General's School; and Chief Prosecutor for the 101st Airborne Division; Encryption, Asymmetric Warfare, and the Need for Lawful Access, 12-1-2017; William & Mary Bill of Rights Journal, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4905083; accessed, 10-21-2025] Aaron

Advocates of the first option may believe that it provides the best protection against privacy compromise, either the result of unlawful government action or private intrusions. However, these advocates may not have fully contemplated the risk that **foreclosing** government **access** to data **through normal, law enforcement**-type modalities may push the **gov**ernment into **pursuing extraordinary surveillance measures justified by** an assertion of **war powers**. There is no reason to expect that the government will **ignore** the potential **security** advantages of surveillance targeted at **"dark spaces**."95 Indeed, the nature of the international **terrorist threats** confronting the nation—threats emanating from organizations that **rely heavily** on commercial **communications** capabilities not only for **command** and **control**, but for **recruiting** and inciting **violent** terrorist

action**s**—virtually **guarantees** that government **counterterr**orism efforts will **constantly seek** to access such data.

Without an ability to rely on normal law enforcement agencies and processes to engage in such surveillance, the **gov**ernment will **not** simply **"give up"** the effort. **Instead**, the **incentive** to **invoke wartime powers** and **utilize all surveillance** capabilities, including **military capability,** will be **increased**. Like the **Bush**-era PSP, a future President would need only determine that the information sought by the government was **related** to an enemy involved in an ongoing **armed conflict** with the United States. And this might not be all that difficult finding to make. First, as has been demonstrated with the seemingly endless expansion of authority derived from the **post-9/11** Authorization for Use of Military Force,96 it has not been terribly difficult to link terrorist organizations to that authority.97 Second, even a presidential determination that a terrorist threat fell beyond the scope of that authorization would not bar a President from invoking **war** powers as a justification for surveillance efforts.98 Because it is now well established that international terrorist organizations may present the United States with a **threat** of an **"armed attack,"** a President would be able to invoke the inherent **constitutional** "defensive" **war power** to disrupt or disable such a threat threats, FISA establishes the sole means for authorizing surveillance.99 But, this is not necessarily an insurmountable obstacle. First, President Bush never conceded a lack of constitutional authority for his program, but simply chose to **acquiesce** to the use of FISA as the means to obtain surveillance authorization.100 Second, FISA may very well provide ample authority to utilize extraordinary measures to penetrate "dark spaces" to include the use of military surveillance capabilities.

The idea that democracy creates peace is unserious---modeling failures, aggressive norm-setting, lack of empirics, AND transition wars.

Walt 10-28 [Stephen M. Walt; doesn't think there's an impact to economic decline and American political scientist serving as the Robert and Renee Belfer Professor of international relations at the Harvard Kennedy School; 10-28-2025; Foreign Policy; "Democratic Peace Theory, R.I.P."; https://foreignpolicy.com/2025/10/28/democratic-peace-theory-r-i-p/; DOA:10-28-2025] auraine

Some social science theories have remarkable staying power; others turn out to have a more limited shelf life. Sometimes a once-promising idea just doesn't seem to lead anywhere—Talcott Parsons's structural-functionalist approach to sociology might be one example—and eventually most scholars abandon it and move on. Or a novel theoretical argument can sound compelling when it first appears, but subsequent research reveals its logical or empirical limitations. In other cases, the real world delivers a harsh verdict on a bold claim—remember the "end of history" thesis?—although some **discredited** theories can survive, zombie-like, because **powerful interests** find it useful to keep them alive.

Why do I bring this up? Because I have recently found myself wondering what exactly has happened to democratic peace theory (DPT). As students of international relations all know, DPT was a major intellectual preoccupation for IR scholars from the mid-1980s until well into the 21st century. Beginning with Michael Doyle's seminal works on the topic (refining arguments originally developed by Immanuel Kant), the idea that "democracies don't fight each other" inspired a vast outpouring of scholarly articles and books, along with a number of important critiques.

In its modern form, DPT **rest**ed on the **empirical observation** that well-established democratic states did not fight wars with each other, a finding that one prominent scholar called "the closest thing we have to an empirical law in the study of international relations." Proponents developed several competing explanations for this intriguing observation, sometimes married with other factors such as economic interdependence. Unlike many social science theories, DPT quickly left the ivory tower and was seized upon by politicians seeking to justify U.S. efforts to spread democracy around the world or to expand institutions like NATO. The theory's seductive appeal was obvious, for it implied that a world made up entirely of **liberal states** would be free from war. As President George W. Bush put it at the beginning of his presidency, "Our goal is to turn this time of American influence into generations of democratic peace."

Not surprisingly, DPT's bold claims attracted no shortage of critics. Some scholars pointed out that the **causal mechanisms** underlying the empirical finding were **inconsistent** and **unconvincing**, while others suggested that the observed infrequency of war between democracies might be a **statistical artifact**, given there were hardly any genuine democracies before **1945**. Others suggested that the absence of war between democracies was due to **power politics**, given that most of the post-**World War II** democracies were part of America's **Cold War** alliance network, or the result of specific coding decisions and shifting definitions of "democracy." Others pointed out that although well-established democracies might not have fought each other in the past, **newly democratizing states** seemed to be **especially war-prone**, which implied that spreading democracy might pay off in the long run, **but** getting there would be a **bumpy process**.

This intellectual battle raged on in the pages of scholarly journals and monographs, and eventually reached something of a dead end, as the results of competing large-N studies became increasingly dependent on the assumptions and modeling techniques being employed. My own view, for what it's worth, is that the more extreme claims for a democratic peace were **overblown**, but democracies might be somewhat less likely to fight each other because it was somewhat harder, though not impossible, for them to overcome public resistance to a war.

More importantly, I thought that DPT did not tell us very much about what a world composed entirely of democracies would be like, because such a world has never existed and absence of war between democracies had been reinforced by the constant presence of potentially dangerous non-democratic rivals. If all autocracies were **replaced** by democracies, however, even Kantian republics might view each other with some suspicion and begin to draw invidious **distinctions** among themselves. Sharing democratic principles does not eliminate all **conflicts of interest**, and might parliamentary and presidential republics begin to see each other as different and possibly **dangerous**? If so, then spreading democracy far and wide might not be the panacea that DPT's most enthusiastic proponents believed. And like some other scholars, I worried that DPT encouraged **powerful democracies** to launch violent **crusades** against illiberal states in the name of peace, and that such efforts would gradually erode **liberal norms** and **freedoms** at home, which is **precisely** what has happened.

Companies already hand over decrypted communications.

Goode '24 [Lauren Goode; Senior Correspondent at WIRED; Michael Calore; Reporter for Consumer Technology at WIRED; 09-05-2024; "Seriously, Use Encrypted Messaging"; WIRED; https://www.wired.com/story/gadget-lab-podcast-657/; access at https://archive.ph/jvPVE; accessed 10-27-2025] leon

Michael Calore: So typically, I know things are probably different in France than they are in the United States, and they're different in every territory, but typically when **law enforcement** goes to a **platform** and they say, "We want the goods on this **list of users** who we can see doing crimes on your **platform**," what's the liability there? What does the platform typically have to provide law enforcement?

Andy Greenberg: Well, typically, they just have to **comply**. I mean, this is the law, that if law enforcement asks for information in your jurisdiction, where you are a legal entity, you have to comply with laws that you hand it over. And Google, Facebook, Twitter, all of **these companies** have to hand over stuff to law enforcement **all the time**. Sometimes they **fight it**, sometimes they go to court on behalf of their users, if they even have an opportunity to fight their requests in court. But generally, this is just the routine that these companies hand over all sorts of cloud data or online data to law enforcement all the time as a part of their investigations. Telegram is based in the UAE. I think that they perhaps thought they could, through a jurisdictional evasion, get away with not complying, but Pavel Durov is even a French citizen. So when he flew to France, he took his life in his hands by having flouted these laws. The ways that communications **platforms** actually **get away** with not complying with those laws usually is just **to say**, "Oh, well, we don't have what you're asking for."

Lauren Goode: Right. That was the case of Apple and the San Bernardino shooting several years ago, basically saying, "Our messaging is so encrypted, we don't even have access to this."

Andy Greenberg: Exactly. Like, “Sorry, we don't even know **what that data** is. It's encrypted. It's **end-to-end** encrypted,” most importantly. That means it's encrypted from one end user to the other with the company in between not even being able to decrypt the information and look at it themselves or share it with law enforcement. That is part of why end-to-end encryption is **so powerful**. It's why Mark Zuckerberg has, at some point, said that he wants to make Facebook—all of Meta stuff, in fact, Instagram, WhatsApp—fully end-to-end encrypted, because then he doesn't have to worry about moderation. He doesn't have to **worry** about these data requests. Of course, it **sounds good** for **privacy** as well, but it also takes a huge legal compliance load off of his company too.

Hacking

2AC---AT: Hacking---General

Lawful access is a legitimate front door that flips privacy, security, inevitable crackdown incentives, & backdoor creation.

Corn ’17 [Geoffrey S. Corn; George R. Killam Jr. Chair of Criminal Law; Director, Center for Military Law & Policy Texas Tech University School of Law. Professor Corn served in the U.S. Army for 21 years, retiring in the rank of Lieutenant Colonel. He served as the Army’s senior law of war expert advisor, tactical intelligence officer in Panama; supervisory defense counsel for the Western United States; Chief of International Law for US Army Europe; Professor of International and National Security Law at the US Army Judge Advocate General’s School; and Chief Prosecutor for the 101st Airborne Division; Encryption, Asymmetric Warfare, and the Need for Lawful Access, 12-1-2017; William & Mary Bill of Rights Journal, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4905083; accessed, 10-21-2025] Aaron

*E2EE = end to end encryption

I. FOURTH AMENDMENT **REASONABLENESS** AND THE BALANCE OF INTERESTS

Assessing the legality of government efforts to surveil “dark” spaces, whether motivated by law enforcement or counterterrorism interests, must begin with the Fourth Amendment. In one of my previously published articles, which has since evolved into a chapter for the book, The Cambridge Handbook of Surveillance Law, I argue that **the Fourth Amendment imposes no barrier to enactment of laws requiring feasible government access to encrypted data**.26 The focus of that chapter evolved from
the substantial public debates surrounding the San Bernardino iPhone “incident.”27 Many critics of the government, including the aforementioned chapter’s co-author, questioned the wisdom and legality of government efforts to demand access codes to the E2EE embedded in the iPhone used by the deceased terrorist in that incident.28

For me, this issue raised the important question of whether the government has the authority to, and ought to, require encryption designers and manufacturers to preserve the means to enable government agents to **lawful**ly access private data stored on the devices they market. While many **critics** of such a proposal lamented the idea of government mandated “backdoor” access to private data,29 I viewed this as a requirement to build into the encryption an actual front door.30

In my view, **backdoor access** connotes **clandestine** or surreptitious **access**.31 This, I argued, is exactly what the government will be compelled to pursue and **exploit** when access through a proverbial **front door is impossible** because there is no **front door**.32 However, by creating a highly **secure front** door, it is possible to achieve a **mutually satisfactory, balanced alternative:**

To be clear, this “split key” proposal is not a subterfuge method of creating backdoor access to data. Unlike a backdoor, which generally refers to an undisclosed vulnerability in an application or device, a front door is a **well-documented** and **clear** mechanism for both **encrypting and decrypting** data, whether it be data in motion (communications) or at rest (stored data). To be secure, encryption should be subject to **rigorous testing**. Thus, its presence should be open to the public and available for attack, both in laboratories and in the real world. This is the only real way to evaluate the trustworthiness of encryption, with vulnerabilities being corrected as they are discovered, to strengthen the protocol and its implementation constantly. Essentially, a front door is the digital equivalent of a big, ingeniously engineered lock on the only entrance to an otherwise secure building. It is a lock that has been **tested** by every available lock picker and found to be secure, with any identified weaknesses being **constantly fixed**. Such a lock is always **superior** to a **secret** entrance in the rear of a building.33

Such front door access would better serve the interests of both privacy and security, as each would be effectively balanced.34 First, by “**splitting**” the encryption key and **entrusting** part of it to a **neutral organization** devoted to **privacy protection**, the individual will be provided enhanced protection by imposing a greater burden on the government to access the key.35 Second, by requiring compliance with normal

Fourth Amendment justifications and **authorizations to engage in surveillance and seizure of any data, the data will be protected with no less vigilance than the protection of the home**.36

Of course, creating a front door will inevitably facilitate government access to private data **when properly and lawfully authorized**. This reality is contrary to the objectives of many privacy advocates.37 Some even argue that such a creation is, in effect, a subterfuge backdoor:

These opponents frame efforts to preserve such access as a call for the creation of "backdoors" that can be exploited by the U.S. and any other government. They argue that the creation of backdoors will introduce unacceptable vulnerabilities in products and systems and point to examples where, in the past, such vulnerability have been exploited by hackers.

As I have argued previously, such a suggestion is shortsighted, as it is this approach that actually further enables exploitation by hackers. 39 **When front door access is eliminated** from E2EE (or any other type of data storage), a determination that access to that data is **necessary** and lawful will compel **gov**ernment agents to work to **identify**, if not **create, backdoor** access.40 In such situations, there are strong incentives for that access to be **clandestine**, because disclosing the access point will in turn **alert** the manufacturer to a vulnerability requiring a security patch.41 It would be unwise for the government to reveal the backdoor, only to then disclose it.42 As a result, an **actual privacy vulnerability**, subject to **exploitation** by non-government actors, may persist.43

Furthermore, it is likely that the government may identify such "backdoor" vulnerabilities even when not engaged in surveillance efforts directed against specific targets as part of overall data protection operations. Without confidence that data access could be facilitated through **lawful** front door access, the government would have a **powerful incentive** not to share this information with the manufacturer or service **providers**. In short, **front door access** incentivizes government cooperation with the private sector to **identify** and **prevent backdoor breaches**, which ultimately **enhances protection** of private data from **unlawful** or unauthorized access.44

Reasonable people will inevitably differ on the proper balance between privacy and public security implicated by encryption technology, as well as how encryption facilitates exploitation of "dark spaces" by dangerous and nefarious actors. However, it is legitimate that a **balance between these interests should be the goal of law and policy makers**. Those who argue that no government effort to ensure lawful access to these dark spaces can be tolerated without sacrificing essential liberty are comfortable with technological creation of impenetrable zones of privacy. While such zones will obviously maximize the protection of privacy from government intrusion, they will do so at a cost. As I argued in my prior chapter, I believe an impenetrable zone of privacy is inconsistent with the underlying rationale of the Fourth Amendment:

Balancing the competing interests of collective societal security and individual liberty is central to the Fourth Amendment touchstone of reasonableness. The notion that the Fourth Amendment provides an individual right to an impenetrable zone of privacy is therefore inconsistent with the text and judicial interpretation of the amendment. Instead, balance remains the operative concept: protection against unreasonable search and seizure inherently acknowledged that the people can be subjected to **reasonable** searches and seizures. In short, the **amendment never imposed an absolute restraint on government surveillance, even when directed against the interests protected by the amendment's text (persons, homes, papers, and effects).** Instead, the people were provided an absolute right to be secure against **unreasonable government intrusions** into those places and things protected by the Fourth Amendment.45

That key constitutional provision certainly does not mandate government action to guard against the creation of such a zone, nor does it require the government to tolerate such zones.46 Thus, from a regulatory perspective, the Fourth Amendment is probably best understood as neutral on the question of whether government should seek to mandate preservation of access to encrypted zones of privacy.47

But what the Fourth Amendment has historically tolerated—reasonable government measures to investigate and discover crime and other threats to public security— should be instructive in this debate.48 Reasonableness, after all, is as the Supreme Court reminds us, the "touchstone" of the Fourth Amendment.49 That touchstone of reasonableness, in turn, is consistently defined by balancing individual privacy with societal interests in effective law enforcement.50 With the exception of dangerous medical procedures to recover evidence from within a suspect's body,51 even the most carefully protected zone of privacy—the home—is subject to government intrusion when properly authorized.52 If the most fundamental source of protection from government intrusion into a citizen's privacy is defined by a reasonable balance between **privacy** and **security**, advancing this **balance** should be the **ultimate objective** of **lawmakers** addressing the difficult question of how to deal with "dark spaces." Requiring preservation of encryption keys to facilitate lawful government access to private data is, in my view, a rational manifestation of this balance of interests. In contrast, allowing for the continued creation and enhancement of technology that seeks to create **impenetrable** zones of privacy **distorts** this balance.

Ultimately, there are only three virtually undeniable constants in this debate.53 First, the **market** will continue to incentivize the **development** of **encryption** technology that frustrates, and ideally prevents, government access to **private communications**.54 Second, while these **innovations** will be **intended** to preserve the privacy of law abiding citizens, the **dark spaces** they create will offer exploitation opportunities for individuals and **groups** engaged in activities that **threaten society**.55 And third, **the gov**ernment will **constantly endeavor** to **access** these dark spaces, precisely because of the **risks** inherent in allowing such exploitation.56 Furthermore, the nature of national security threats, most notably terrorist threats targeting the U.S. homeland, have magnified the government's interest in penetrating these spaces.57

II. ASYMMETRY AND THE ADAPTIVE ENEMY

Concern over feasible access to encrypted communications is no longer simply a question of balancing privacy against the interests of effective law enforcement. Today, the risks attendant with "dark space" communications transcend criminal threats and are inextricably intertwined with counterterrorism efforts.58 This should come as no surprise. The **United States is engaged in an ongoing armed conflict against multiple transnational terrorist organizations.**59 While the notion that response to this threat qualifies as an armed conflict remains controversial for many international law experts, the fact remains that the **U.S. perceives** the nature of the threat posed by both **al-Qaeda** and **ISIS** as transcending that of ordinary criminal activity.60 Instead, the **national decision** to treat the **ongoing battle** against these **threats** as an **armed conflict** indicates a **willingness** to use **expanded means** and legal **authorities** to disrupt and disable these groups.61

Of course, these enemies do not engage in and employ analogous debates or handwritings over the appropriate legal framework for their terrorist activities. Instead, they embrace tactics that constantly seek to exploit enemy vulnerabilities in order to offset the superior material and information capabilities of their opponents—a phenomenon characterized by the term, "asymmetric warfare."62 Interestingly, there is no consensus definition of asymmetric warfare.63 However, as the following summary indicates, it generally refers to conflict between conventionally disparate enemies, with the inferior enemy seeking to offset its weakness by identifying and exploiting vulnerabilities of the conventionally superior opponent: Asymmetric warfare is generally understood to be a conflict in which the strengths and sizes of the opponents do not mirror each other. The side with the conventional disadvantage is probably incapable of winning through direct, conventional warfare. It must seek victory through other methods that exploit weaknesses in the superior conventional power's capacity to prevail. Examples include the Maoist Peoples' War against the Imperial Japanese Army, the Vietnamese dau trahn strategy in the First and Second Indochina Wars, and al-Qaeda's tactics in the WOT [(War on Terror)].64

So characterized, there is nothing new about asymmetric tactics, which have been part of military theory and doctrine dating back to the writings of Sun Tzu.65 However, the struggle against today's transnational terrorist threats has resurrected the focus on how to effectively address asymmetric threats, threats that challenge our national security capabilities well beyond the "battlefield." 66 A Rand Report explains the characteristics and challenges associated with this modern permutation of asymmetric warfare:

<<<TEXT CONDENSED FOR READABILITY NONE OMITTED>>>

The legal dimension of asymmetric warfare is often called "lawfare." This is a relatively new area because the nature of modern warfare has changed dramatically from that of the "classical" wars of the past. In classical warfare, the enemy is visible, and soldiers are easily identifiable by uniform and openly carry weapons. The use of lawfare is part of the larger pursuit of legitimacy. By contrast, in asymmetric warfare, the enemy is usually invisible, hiding among the civilian population, often in densely populated areas. Lethal attacks are often launched from civilian facilities. There may be no means to distinguish combatants from the civilian population. In classical warfare, a democratic nation's obligation and responsibility is to conduct the war according to the rules of war— especially the principle of distinction between combatants and civilians. When it comes to asymmetric warfare, the opponent often targets civilians, not only ignoring the rules of war but deliberately doing so as part of an overall strategy against the democratic state. In classical warfare, the ultimate goal of both sides is to defeat the enemy with respect to its capabilities to use military power. In asymmetric warfare, the opponent's goal is not to defeat the state's armed forces but rather to make the civil society so terrified and concerned that it will pressure politicians to withdraw from the state's positions or abandon its policy aims, thereby losing the war not through the battlefield but through determination of the democracy not to continue fighting. In classical warfare, the territorial and temporal limits of the conflict are relatively defined. The nature of asymmetric warfare is much more amorphous. It is not limited to a certain territory or distinct timeline. In classical warfare, the enemy's fighters are essentially anonymous: It is not important to know the name of the enemy's soldier or commander before attacking him. When it comes to asymmetric warfare, in many cases, it is crucial to know the opponent and to have very personal and detailed information as a precondition for determining the legitimacy of a strike. These new features are different from the set of assumptions that were the basis for the laws of war, especially international humanitarian law. These laws are the basis of the legal norms, binding democratic nations to conduct their military power accordingly. This differentiation, combined with the emerging power and influence of international tribunals, is known as lawfare. Lawfare is often used as a negative term, suggesting manipulation, although it is not limited to that. Ironically, it is an area in which the democratic state and its officials feel vulnerable. In contrast, the opponent often deliberately violates the norms while simultaneously using them to weaken democratic nations. Lawfare is used to counter the weapons of the democratic state by exploiting its own laws and judicial systems. It focuses on government and personal liability. Because asymmetrical warfare takes place in densely populated areas, it inevitably generates more grounds for legal action. While nonstate adversaries typically do not comply with international humanitarian law, as already noted, they will simultaneously use that law to undermine the motivation and legitimacy of their democratic state foes. . . . There are inherent difficulties in applying the norms of international humanitarian law to asymmetric warfare. Applying the concept of proportionality is next to impossible and provides no guidance to the commanders on the ground, since it comes without clear guidelines. It is also difficult to apply the fundamental principle of distinction in a civilian environment, since the entire battlefield is often a civilian area, making it nearly impossible to distinguish between combatants and civilians. Moreover, the application of the principle of military necessity is problematic when it relies heavily on intelligence and other secret evidence. Finally, asymmetric warfare presents challenges to efficiently striking the opponent without violating the principle of perfidy. Effective

warning—for example, roof knocking—weakens the chances of a successful military mission and places soldiers at additional risk. Other challenges include striking political or religious targets, regardless of whether they are also being used to support active military operations. What about individuals like Hamas leader Ismail Haniye? Or how should armies treat bridges or electricity? In World War II, such targets were bombed for obvious military reasons. In asymmetric warfare, they may be considered civilian facilities. Consequently, the challenge is how to adjust international humanitarian law to apply to modern asymmetric wars. There needs to be legal recognition of the constant state and timeless nature of armed conflict against nonstate adversaries. There needs to be legal application of the principle of self-defense against nonstate adversaries when there is no other alternative (for example, in failed states). Given that liberal democracies are often on the front line in the fight against nonstate adversaries, there needs to be a flow of information among them as well. Furthermore, it is necessary to acknowledge the role that intelligence plays in winning the war and to determine the "military necessity" and the key element of intelligence for the principle of distinction. Also, wider legal tools and wider public control over intelligence agencies should be considered. It is important to develop a publicly available code of conduct for certain military actions, such as targeted killings. It is important to know who is making the decisions and under what guidelines and circumstances targeted killings are allowed. Sharing more intelligence publicly assists in efforts to win the imagefare battle.67 As indicated in the RAND Report, one aspect of asymmetric terrorist tactics that creates especially difficult challenges for law-abiding nations is exploitation of the law to gain tactical advantage.68 Whether on a conventional battlefield in Iraq, an unconventional battlefield like Afghanistan, or the enemy's "homeland," contemporary enemies look for opportunities created by their opponent's compliance with legal obligations.69 This aspect of asymmetry may not be completely new, but it is more pervasive than ever before.70 This may be a consequence of the increasing role law plays in defining the legitimacy of national security actions. In fact, the concept of legitimacy is now included in some U.S. military doctrine as a principle of war, alongside such time-tested principles as mass, offensive, and economy of force.71 As a result, democracies face an increasingly difficult challenge of developing and implementing national security policies that are effective, not only in the immediate sense of achieving the effect on the opponent, but also in the sense that they manifest the type of commitment to law that is central to the notion of legitimacy.

<<<LINE BREAKS CONTINUED>>>

This aspect of asymmetry intersects directly with the issue of government surveillance access to "dark spaces." **Remotely radicalized, homegrown terrorists** are assessed as among the most significant terrorist threats faced by Western nations.72 Furthermore, attacks in Paris, Brussels, and other major cities demonstrate the risk of small, well-organized attack cells operating in relative plain sight.73 Whether it is a **lone wolf**, or a small **cell** of organized **operatives**, communication is obviously **essential** for their **success**. And, because it is no mystery that the government is constantly seeking to identify and preempt terrorist attacks, it must be **self-evident** to such individuals that identification and exploitation of **dark** communication **zones** will **substantially** enhance their **likelihood of success**. Investigations into several attacks, such as the **ISIS Paris** bombings and the **Brussels** airport bombing, indicate that operatives relied on **WhatsApp** for vital **communications.** 74

The ready **availability** of **E2EE** with no built-in **front door** access will almost **certainly** be viewed by those engaged in **terrorist**ic activities as the **communication**s **method** of choice. Like all aspects of asymmetric warfare, they will seek to exploit what is viewed as a self-inflicted vulnerability to the maximum extent. The **more confident** they are in the **immunity** of their communications **from timely government surveillance**, the more likely it is they will rely on such dark spaces. But this also means that the government is all that more likely to increase efforts to **penetrate** such spaces. And this really frames the ultimate question in the encryption debate: does increasing the difficulty of lawful government access ultimately advance or compromise legitimate privacy interests? The answer to this question may be derived in part from the multipronged legal framework the U.S. relies on for counterterrorism operations.75

Companies will innovate solutions.

Joris Van **Hoboken 14**, Professor of Law at Brussels School of Governance, Associate Professor at the Institute for Information Law, "Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era," Hein Online, xx/xx/2014, https://heinonline.org/HOL/Page?handle=hein.journals/maine66&div=24&collection=journals, tristan

IV. CLOSING BACKDOORS AND SHAPING FRONT-DOORS

When looking at the measures discussed in the previous Section, it becomes clear that there are technical possibilities to design cloud services in ways that limit the ability of cloud providers to access the data of their customers. This Article takes the position that the ongoing **discussions** over cloud **security** and the increased worries over transnational **surveillance** are likely to spur further **innovation** and subsequent adoption of such solutions in the marketplace.

High-security demanding customers such as government agencies and corporate and organizational users with particularly strict demands for information security are likely to drive these market responses.214 Customers will **insist** upon better **guarantees** of **security** and **confidentiality** and may **refuse** to do business with popular, U.S.-based cloud services subject to far-reaching government surveillance powers. Indeed, they may be barred from doing so under new proposals in Europe and elsewhere requiring their citizens to rely on local cloud services.215 In the market for individual users of cloud resources, there may generally be an **increasing demand** for better **security** and **privacy** safeguards as a result of the widely discussed examples of mass surveillance of online interactions and communication. In addition, law and regulation may increasingly require that certain types of disproportionate lawful access to cloud data be excluded if cloud providers want unrestricted access to the market.

T-Attackers USE encryption to coordinate---access solves.

Toulas ’24 [Bill Toulas; infosec news reporter @ BC; 12-3-2024, "Police seize Matrix encrypted chat service after spying on criminals," BleepingComputer, https://www.bleepingcomputer.com/news/security/police-seize-matrix-encrypted-chat-service-after-spying-on-criminals/, accessed: 10-12-2025] william

An international law enforcement operation codenamed 'Operation Passionflower' has shut down **MATRIX**, an **encrypted** messaging platform used by **cybercriminals** to **coordinate** illegal activities while **evading police**.

It should be noted that MATRIX is a different entity from the secure open-source, decentralized, real-time communications protocol with the same name, which is perfectly legal to continue using.

The operation was conducted across **Europe**, including France, the Netherlands, Italy, Lithuania, Spain, and Germany, and was coordinated by Europol and Eurojust.

A **crime enabler**

The police tracked down MATRIX after recovering the phone of a shooter who attempted to assassinate journalist Peter R. de Vries in July 2021.

After analyzing the phone, they discovered it was customized to connect to an encrypted messaging service called Matrix.

A joint investigation team (JIT) between the Dutch and French authorities allowed the **police** to **monitor** and intercept **2.3 million** messages in 33 different languages sent through the devices. However, no technical details were provided on how they could do so.

"For **three months**, authorities were able to **monitor** the messages from possible criminals, which will now be used to **support** other **investigations**." reads an announcement by Europol.

"During a coordinated operation supported by Eurojust and Europol, the messaging service was taken down by Dutch and French authorities and follow-up actions were executed by their Italian, Lithuanian and Spanish counterparts."

MATRIX's **40 servers** spread across Europe facilitated the **communications** of at least **8,000** user accounts, who paid between $1350 and $1700 in cryptocurrency for a Google Pixel-based device and a six-month subscription to the service installed on the phone.

Pre-E2E adoption thumps.

Eric **Manpearl 17**, Senior Fellow at the Robert S. Strauss Center, J.D. from the University of Texas School of Law, M.A. from Lyndon B. Johnson School of Public Affairs, B.A. from Rice University, “Preventing 'Going Dark': A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate,” SSRN, 11/15/17, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3068578, tristan

Benjamin Wittes, a senior fellow at the Brookings Institution and cofounder of Lawfare, has raised the point that **major** Internet companies currently have the ability to **decrypt information**.1 42 Google has the ability to **decrypt Gmail** and Gchat communications because this allows Google to target users for advertisements. 1 4 3 Also, Gmail is able to **filter spam**, which can contain malware, because Google can read emails ‘plaintext, which would not be possible with end-to-end encryption. Further, Google offers the full text search of files stored in the cloud, which requires access to plaintext, too, and could not occur with end-to-end encryption. 14 5 There have **not** been **security issues** with Google's services thus far. 14 6 Despite a lack of security problems, Google has announced that it will offer a messaging application, Allo, that will use opt-in (not default) end-to-end encryption, and video calling application, Duo, that will use default end-to-end encryption. 14 7 Facebook's Messenger used to be able to be **decrypted** by Facebook.1 4 8 Although the company has started testing opt-in (not default) end-to-end

encryption for Messenger, Facebook has **not** indicated this move is because the service was insecure. 14 9 In addition, Apple continues to enable **iCloud backups** to occur in a manner that can be **decrypted**. Once again, there have **not** been **security issues** with the service."5 Thus, there does **not** seem be evidence that these major Internet companies' services are insecure because they have the ability to **decrypt** information. Some of the fears of insecurity seem to actually stem from a disdain for lawful surveillance. However, lawful surveillance is not a cybersecurity risk.

2AC---AT: Alternatives Solve

Alternatives fail.

Mack 20 [William Mack; Master of Arts in Security Studies; Naval Postgraduate School; "The Key to Lawful Access: An Analysis of the Alternatives Offered in the Encryption Debate"; pp 86-87; https://apps.dtic.mil/sti/citations/AD1126508; DOA:11-19-2025] auraine

E. CONCLUSION

While this thesis has examined the alternatives individually, some of the literature on the subject suggests that the alternatives should be viewed in unison. That is, policy going forward should maintain that all these alternatives should be implemented instead of just a singular option as the solution. Where one alternative is not successful, another may be. When lawful hacking does not result in accessing a device, for example, collecting metadata may provide investigators and prosecutors with the evidence they need to move forward. However, as the analysis and the case studies **illustrate**, these alternatives have **too many drawbacks** even when grouped as a **whole** because **none** can ensure **complete** access to the content that law enforcement needs.

Another gauge of the **effectiveness** of these alternatives in totality is that government **agencies are already** using **all** the alternatives yet still **sounding the alarm** for lawful access because of the challenges it **continually faces** in decrypting data. While these options are offered as alternatives to lawful access, they already serve as methods for investigation and intelligence collection on a regular basis, and are often fruitful methods as well. However, the case studies illustrate that in many instances, these methods are **ultimately ineffective** at granting agencies the **range of access** to the content of communications and mobile devices that those agencies need.

Empirics prove.

Economist 24, British News Organization, "The largest sting operation you've never heard of," The Economist, 7/16/24, https://www.economist.com/culture/2024/07/16/the-largest-sting-operation-youve-never-heard-of, tristan

In 2018 the FBI went one better with Operation Trojan Shield. "Dark Wire" by Joseph Cox, a technology journalist and the co-founder of 404 Media, a website, tells the story of how American and Australian officials quietly established **Anom**, an **encrypted messaging service**, to **attract criminals** seeking to **evade surveillance** on traditional platforms.

The app promised **whizzy features**, such as messages that would **auto-delete** and the ability to send voice notes that scramble a user's voice. In reality, all the data was **funnelled** to a server in Lithuania, which was an open book to the **FBI**. The **result** was an intelligence bonanza, with the FBI processing as many as 1m messages a day in 45 languages. That led to the arrest of more than **1,000 people** and the seizure of **hundreds** of firearms by the time the operation was wound up, and the subterfuge revealed, in 2021. It was the **largest** law-enforcement **sting operation ever**.

Mr Cox, who spent years doggedly tracking the story and getting to know its players, many of them unsavoury international gangsters, has written a vivid account of the saga. The pages pop with dramatic irony: criminals **trade cocaine** and **confess** to lurid **murders** in the belief that their **incriminating texts** and messages are safe from prying eyes. One agent confesses "chuckling to myself, as these guys in whatever foreign country are going back and forth, talking about the FBI".

Drug smugglers and hitmen speak for themselves, their personalities memorably captured by their own messages. Maximilian Rivkin, known as "Microsoft", a sociopathic Swedish polyglot, plots crimes in Croatian, English, Spanish and Swedish. "He punctuated his assassination plans with heart and thumbs-up emojis," writes Mr Cox. At one stage, Mr Rivkin requests a bulk discount for ordering multiple murders at once.

"Dark Wire" conveys the moral ambiguities and grubby trade-offs inherent in this sort of intelligence work. "The FBI was happy to allow some crimes to play out…if it meant collecting intelligence on other ones," writes Mr Cox. "Some crimes ultimately weren't worth burning the

entirety of Anom over." On around 150 occasions the FBI had to intervene to stop a threat to life, passing on details of murder plots to local authorities around the world, often disguising the source of the intelligence.

The book also raises deeper questions about the nature of secrecy, privacy and the law. If you want to communicate securely with someone without others eavesdropping, it makes intuitive sense to choose a device optimised for that purpose, such as Anom. The problem is that the people who go to such lengths to communicate privately often tend to be those who have something to hide, such as spies or criminals. Those devices, like Crypto AG machines before them, thus become particularly attractive targets for intelligence agencies and police forces. That, at least, is how it used to work.

Nowadays **"end-to-end"** encryption—the method of enciphering your messages so that they look garbled to anyone who should intercept them en route—is **widely available** on apps such as Meta's WhatsApp, Apple's iMessage and Signal. The result is that criminals and law-abiding citizens mingle on the same platforms.

Mr Cox says that security agencies see "large-scale, **bulk interception** missions" like Operation Trojan Shield as the **future** of the fight against **organised crime**. But can they pull off such a big coup again? Criminals will no doubt be warier of digital Trojan horses.

Military

2AC---AT: Military

Military systems are distinct.

Eversden '21 [Andrew Eversden, graduate of American University. 8-11-2021, "US Army awards $774 million encryption device contract", Army Times, https://www.armytimes.com/battlefield-tech/it-networks/2021/08/11/us-army-awards-774-million-encryption-device-contract/, doa 10-31-2025] //ALuo

WASHINGTON — The U.S. Army chose Sierra Nevada Corp. and General Dynamics Mission Systems to build its next-generation encryption device that will secure the joint force's future tactical network, the service announced Wednesday.

The two companies will participate in the development, production and sustainment of the Next Generation Load Device-Medium, a cryptography tool to secure the service's network from adversaries' cyber and electronic warfare threats. The contract, worth up to $774.2 million over 10 years, was awarded by Program Executive Office for Command, Control, Communications-Tactical.

The advanced cryptology device that will replace the Army's legacy Simple Key Loader devices. The new capability will allow network managers to reconfigure cryptographic products, remotely download new software and improve operational environment awareness, according to a PEO C3T press release.

"The NGLD-M will enable delivery of the strongest NSA-generated cryptographic keys to tactical, strategic, and enterprise network systems operating from secret to the highest levels of security classification," said Paul Mehney, communications director for PEO C3T. "Through over-the-air capability, modern cryptographic algorithms will be transferred by NGLD-M to counter the threats posed by increased proliferation of adversarial cyber and electronic warfare."

The vendors will share an initial $74 million award for development and low-rate initial production, scheduled for fiscal 2024 along with an operational test.

Full-rate production of the encryption device will begin in fiscal 2025 with up to 265,000 products fielded. Once in production, the loaders will be available by units across the services, federal government and foreign military partners. The Army expects to stick with its multivendor approach through the production process and could add vendors in the future as industry capabilities mature, Mehney said.

"NGLD-M will be the biggest materiel change in cryptographic key delivery in twenty years," Michael Badger, product lead communications security, said in a statement. "It will transform COMSEC both in the strength of keys NGLD-M can handle and in the security of its delivery mechanisms."

The release of the NGLD-M request for proposals was delayed last summer after the Army decided to adjust its acquisition strategy. The RFP was released in November.

2AC---AT: Quantum

China's ahead. Postdates.

Riggi '25 [Justin Riggi, 9-23-2025, "How China Is Outperforming the United States in Critical Technologies", ITIF, https://itif.org/publications/2025/09/23/how-china-is-outperforming-the-united-states-in-critical-technologies/, doa 10-26-2025] //ALuo

China has **emerged** as the **leading global power** in the creation of emerging technologies, **dramatically outperforming** the United States in the **vast majority** of critical technological fields. A **key indicator** of this is that China is **dominating** the United States when it comes to **scientific publications**.

This is concerning as it threatens to erode U.S. leadership across the innovation landscape. ITIF conducted a comprehensive analysis of China's innovation capabilities last year, and that research concluded that China's strategic, **state-backed scientific advancement** across **advanced sectors**—driven by **bold industrial policy**, **generous government subsidies**, and **ecosystem integration**—has resulted in a surge of global patents, indicating it has transitioned to become a global innovation leader. China is demonstrating dominance in robotics, leading in battery supply, innovating public health by doubling clinical biotech trials, **outpacing** in **quantum** communication with a **1,200-mile QKD** corridor, experiencing near-peer achievement in AI output, and narrowing gaps in semiconductors and chemicals.

Similarly, according to the latest findings from Australian Strategic Policy Institute's (ASPI) Critical Technology Tracker, which evaluates 64 critical technology categories across 8 domains (e.g., artificial intelligence and robotics), show that China leading in 57, while the United States leads in only 7 technology sub-categories. This is concerning because these critical technologies are the key input to advanced sectors that China is quickly overtaking.¶ When evaluating the top 10 percent of high-quality scientific publications, ASPI finds that China surpasses the United States across all 8 critical technology domains. The gap is particularly pronounced in the energy and environment domain, where China accounts for 46 percent of top-tier publications compared to just 10 percent for the United States. Despite U.S. leadership in AI, China produces more top publications, contributing 30 percent versus 18 percent for the United States. (See figure 1.)¶ Figure 1: Share of the top 10 percent of quality publications across eight critical domains¶ China's dominance is even more evident at the subdomain level. Across the 64 subcategories, there are multiple areas in which China leads the United States by more than 50 percentage points in their respective shares of the top 10 percent of publications. For example, China leads by 60 percentage points in hypersonic detection and tracking technologies. It holds a 56 percentage point lead in high-specification machining processes, which is a key component of advanced manufacturing. (See figure 2.)¶ Figure 2: Subfields in which China's share of the top 10 percent of quality publications is more than 50 percentage points greater than the U.S. share¶ Fortunately, there are some areas where the United States retains a lead over China. In 7 of the 64 critical technology categories, American researchers produce a higher share of the top 10 percent of quality publications. Notable advantages include vaccines and medical countermeasures, quantum computing, and atomic clocks—all areas where the United States leads by at least 10 percent. Furthermore, smaller U.S. leads exist in natural language processing, genetic engineering, nuclear medicine and radiotherapy, and small satellites. (See figure 3.)¶ Figure 3: Subfields in which the U.S. share of the top 10 percent of quality publications is greater than China's share¶ Additionally, ASPI identifies 24 technologies at high risk of becoming monopolized by China and another 19 at medium risk. This assessment is based on China's share of the world's top 10 research institutions and its publication lead over the next-closest competitor. Many of the high-risk technologies have clear defense applications, such as radar, advanced aircraft engines, drones, swarming and collaborative robots, and satellite positioning and navigation. (See table 1.)¶ Table 1: Technologies at risk of becoming monopolized by China according to ASPI

China's progress is the result of **decades-long investments** in **education** and **research** aimed at **building technological capability**. These investments are now yielding **significant returns**, with **implications** for **military**, **economic**, and **scientific** leadership. China's aggressive talent recruitment programs, such as the Thousand Talents Plan, have successfully lured foreign-educated science and technology experts to help accelerate progress in specific industries, particularly semiconductor manufacturing. Furthermore, China's heavy emphasis on STEM education has led it to award more STEM degrees than any country in the world—more than four times the number awarded in the United States.

Importantly, the Chinese government has also established **strong linkages** between **academia**, **industry**, and the **military** as part of its "**Military-Civil Fusion**" strategy. By eliminating institutional barriers between the civilian and military sectors, China has **stimulated** the **rapid development** of emerging technologies in service of its **national defense** and **strategic** ambitions.

Critical infrastructure isn't online---can't be hacked.

Flaherty '19 [Kate O'Flaherty, cybersecurity and privacy journalist @ Forbes, 7-3-2019, U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks, Forbes, https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/, Willie T.]

The U.S. Government has announced a surprising move to secure power grids by using “retro” technologies. It comes after numerous attempts by foreign actors to launch cyberattacks on so-called critical national infrastructure (CNI).

Nations have been trying to secure the industrial control systems that power CNI for years. The challenge lies in the fact that these systems were not built with security in mind, because they were not originally meant to be connected to the internet.

It is with this in mind that the U.S. has responded with a new strategy: rather than bringing in new technology and skills, it will use analog and manual technology to isolate the grid's most important control systems. This, the government says, will limit the reach of a catastrophic outage.

"This approach seeks to thwart even the most sophisticated cyber-adversaries who, if they are intent on accessing the grid, would have to actually physically touch the equipment, thereby making cyberattacks much more difficult," said a press release as the Securing Energy Infrastructure Act (SEIA), passed the Senate floor.

Neg Brief

AI

The U.S. leads the AI race, but China's right behind.

Schnedler 25 [Christian (leader in cybersecurity innovation), Duyane Norman (author and speaker within the Intelligence Community on innovation), 10-27-2025, "Winning the Innovation Race: Why America's Allies Are the Key to Beating Beijing", The Cipher Brief, https://www.thecipherbrief.com/us-china-tech-race, accessed 10-30-25] wrong

Precision U.S. airstrikes against Iran's nuclear program last June demonstrate American technological prowess built on decades of 20th Century Cold War Era investment and innovation. Today, the U.S. continues to originate new technology, yet it finds itself in a race with rivals such as China and Russia to dominate AI, quantum computing, robotics, semiconductors, cyber, and other frontier technologies poised to define global leadership in the 21st Century.¶ To prevail and prosper in this new geopolitical struggle, the U.S. must build and maintain networks of investors, customers, and collaborators among allies with common values and interests. By forging such networks, the U.S. can accelerate the technology innovation and implementation velocity crucial to outpacing its rivals and their formidable manufacturing capacity, human talent base, and financial resources.¶ Opportunities (and Risks) of Buyer Alliances¶ Much of Washington's bipartisan consensus on the necessity of American technology leadership has rightly focused on the nation's capacity to "build the future" at home, safely beyond China's sphere of predation in East Asia, creating American jobs and national wealth, and on terms that ensure these technologies reflect American values.¶ National innovation initiatives, such as the CHIPS Act, support domestic production of advanced semiconductors, and the Trump and Biden Administrations have rightly advocated robust domestic AI innovation initiatives within our own borders.¶ But the other side of the 21st Century innovation race is a sprint to forge strong alliances abroad, with buyers who will accelerate domestic efforts by investing in, buying, deploying, and fine tuning U.S. innovations at a greater scale and profit than would ever be possible were U.S. builders limited to merely selling to U.S. government agencies and corporations at home.¶ Numerous U.S. allies and potential allies in Europe, Asia, the Middle East, and beyond share security concerns about aggressive states such as China, Russia, Iran, and North Korea, and many share U.S. concerns related to the economic, intelligence, and security implications of future dependence on technologies developed in China.¶ While Chinese-based technology builders such as Huawei and DeepSeek have potential to outpace U.S. competitors in the coming years, the Western innovation ecosystem continues to produce the finest and greatest variety of technology solutions. By leveraging allied investments in new digital infrastructure and national security, U.S.-based technology builders can assert their industrial advantages over Chinese competitors in quality, variety of options, and open standards to enable these states to implement the technologies they require to modernize, while protecting themselves from aggression and maintaining their digital sovereignty.¶ Should the U.S. fail to forge these essential partnerships, Chinese rivals will outflank America's technology builders, penetrate and gain permanent footholds in foreign markets, and establish global technology hegemony over the world's frontier technologies, and the future.¶ A Common Defense of Buyer Alliances Strengthens US National Security¶ These technology buyer partnerships are not merely about hardware and software sales, market penetration, technology jobs, and reinvestment of newly created wealth at home. By deploying U.S. national security technologies across a wide range of allies abroad, the cost of building, maintaining, and enhancing them at home will decline as their efficacy, lethality, and capacity to deter aggression will surge.¶ It was the open markets of globalization that enabled Chinese firms to build up tremendous commercial manufacturing capacity in everything from electric cars to computing and telecommunications systems, robotics, ships, pharmaceuticals, and drones. The CCP has leveraged this manufacturing capacity and technical expertise to build new military technology capabilities to threaten the U.S. and its allies. China's dual-use manufacturing capacity is on vivid display in Ukraine, where the country's warfighters favor inexpensive, highly-functional drones built with components manufactured in China.¶ U.S. cybersecurity, AI, and defense tech software technologies are only as impactful as their feedback loops—their capacity to ingest massive amounts of threat and performance data in order to learn and improve their defensive capabilities moving forward.¶ In the same way U.S. drone technologists are observing and learning how drones are performing (and under-performing) in contested Russia-Ukraine battlefield environments, deploying American security technologies along all fronts of geopolitical conflict will make U.S. defenses at home smarter, faster, more creative, more autonomous, and more lethal based on their ability to learn how our adversaries are operating and understanding the weapons and tactics they are likely to use against America's military and homeland.¶ Finally, establishing U.S. technologies' dominance in more countries ensures the U.S. will define technology standards as they are adopted more broadly. As they are adopted, the U.S. and its allies are in a better position to collaborate, surge resources as needed, and execute to resolve threats faster in times of tremendous crises.¶ The Race Ahead¶ We applaud the Trump Administration's efforts to build on existing domestic "technology builder"

initiatives by opening new markets for buyers of American frontier technologies. This "technology buyer" diplomacy was on display in April when President Trump, accompanied by leading technology executives from OpenAI, Nvidia, and others, visited members of the Gulf Cooperation Council (GCC) to establish substantial technology partnership deals. We strongly support the Administration's efforts to negotiate sector-specific partnerships in AI, semiconductors, cybersecurity, and rare earths supply chains with NATO, the EU, Japan, South Korea, India, Taiwan, Ukraine, Australia, and others.¶ Winning the 21st Century innovation race will ensure America's long-term national security, economic prosperity, and freedom to determine its own destiny. Policymakers have achieved a rare consensus that existential geopolitical rivalries demand the US maximize the unique strengths of its private sector with public sector advocacy and investment at home. But because the geopolitical struggle with China and others is global and the stakes of the competition so high, America must forge partnerships that accelerate its investments and efforts at home to effectively meet the challenges confronting her abroad.

Voting affirmative hinders competitiveness.

Levine 25 [Joshua (research fellow in technology policy @ the Foundation for American Innovation), "AI, Encryption, and Data Flows: Policy Imperatives for U.S. Leadership," The National Interest, 02-26-2025, https://nationalinterest.org/blog/techland/ai-encryption-and-data-flows-policy-imperatives-for-u-s-leadership, DOA 10-22-2025] abhi

Avoid Regulations Undermining End-to-End Encryption¶ Cybersecurity is an increasingly important paradigm for lawmakers interested in protecting the American public as well as competing in geopolitical competition with China. End-to-End Encryption (E2EE), a type of messaging that ensures information sent between two parties is private from everyone but the two exchanging parties, is vital to protecting non-public information and ensuring individual privacy. A rash of cyberespionage operations conducted in recent years by state-sponsored hacking groups aligned with nations such as China, Iran, and Russia, as well as independent groups interested in extorting public and private actors, have put millions of Americans' personal information at risk. Such operations have also created vulnerabilities in critical infrastructure around the country, leading the US government to recommend private encrypted messaging services for official business. ¶ At the same time, legislative efforts in the US and abroad, most recently in the United Kingdom, have attempted to force software providers to create "backdoors," for law enforcement to access encrypted networks to prevent the use of such tools for illegal means. While these proposals are looking to solve a serious problem, the second-order effects of destroying E2EE would be significant. This would make millions of Americans and people around the world more vulnerable to cyber attacks. Undermining digital tools that can be trusted to support American digital security, anonymity, and privacy would be a boon to our Chinese competitors, not to mention other nations that would benefit from American companies' and government actors' weaker information security. Domestically, state and federal lawmakers should not advance legislation that would undermine services that utilize E2EE. Globally, the United States should dissuade foreign governments from passing laws that would require American firms to create backdoors into encrypted services.¶ Strengthen Agreements Related to Cross-Border Data Flows¶ Access to high-quality training data is an imperative for continued development of AI models for private and public-sector use.

Chinese tech dominance results in nuclear.

Kroenig 21 [Matthew; Winter; professor of government and foreign service at Georgetown University and the director of the Scowcroft Strategy Initiative at the Atlantic Council; Strategic Studies Quarterly, "Will Emerging Technology Cause Nuclear War?: Bringing Geopolitics Back In," Vol. 15, Issue 4, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-15_Issue-4/D-Kroenig.pdf, DOA 04-18-2025] wrong

If Moscow acquired a newfound ability to more easily invade and occupy territory in Eastern Europe, for example (or if Putin believed Russia had such a capability), it is more likely Russia would be tempted to engage in aggression. Likewise, if China acquired an enhanced ability through new technology to invade and occupy Taiwan or contested islands in the East or South China Seas, Beijing's leaders might also find this opportunity tempting. If new technology enhances either power's anti-access,

area-denial network, then its leaders may be more confident in their ability to achieve a fait accompli attack against a neighbor and then block a US-led liberation. These are precisely the types of shifts in the balance of power that can lead to war. As mentioned previously, the predominant scholarly theory on the causes of war—the bargaining model—maintains that imperfect information on the balance of power and the balance of resolve and credible commitment problems result in international conflict.52 New technology can exacerbate these causal mechanisms by increasing uncertainty about, or causing rapid shifts in, the balance of power. Indeed as noted above, new military technology and the development of new operational concepts have shifted the balance of power and resulted in military conflict throughout history. Some may argue emerging military technology is more likely to result in a new tech arms race than in conflict. This is possible. But Moscow and Beijing may come to believe (correctly or not) that new technology provides them a usable military advantage over the United States and its Allies and partners. In so doing, they may underestimate Washington. If Moscow or Beijing attacked a vulnerable US Ally or partner in their near abroad, therefore, there would be a risk of major war with the potential for nuclear escalation. The United States has formal treaty commitments with several frontline states as well as an ambiguous defense obligation to Taiwan. If Russia or China were to attack these states, it is likely, or at least possible, that the United States would come to the defense of the victims. While many question the wisdom or credibility of America's global commitments, it would be difficult for the United States to simply back down. Abandoning a treaty ally could cause fears that America's global commitments would unravel. Any US president, therefore, would feel great pressure to come to an Ally's defense and expel Russian or Chinese forces. Once the United States and Russia or China are at war, there would be a risk of nuclear escalation. As noted previously, experts assess the greatest risk of nuclear war today does not come from a bolt-out-of-the-blue strike but from nuclear escalation in a regional, conventional conflict.53 Russian leaders may believe it is in their interest to use nuclear weapons early in a conflict with the United States and NATO.54 Russia possesses a large and diverse arsenal, including thousands of nonstrategic nuclear weapons, to support this nuclear strategy. In the 2018 Nuclear Posture Review, Washington indicates it could retaliate against any Russian nuclear "de-escalation" strikes with limited nuclear strikes of its own using low-yield nuclear weapons.55 The purpose of US strategy is to deter Russian strikes. If deterrence fails, however, there is a clear pathway to nuclear war between the United States and Russia. As Henry Kissinger pointed out decades ago, there is no guarantee that, once begun, a limited nuclear war stays limited.56 There are similar risks of nuclear escalation in the event of a US-China conflict. China has traditionally possessed a relaxed nuclear posture with a small "lean and effective" deterrent and a formal "no first use" policy. But China is relying more on its strategic forces. It is projected to double—if not triple or quadruple—the size of its nuclear arsenal in the coming decade.57 Chinese experts have acknowledged there is a narrow range of contingencies in which China might use nuclear weapons first.58 As in the case of Russia, the US Nuclear Posture Review recognizes the possibility of limited Chinese nuclear attacks and also holds out the potential of a limited US reprisal with low-yield nuclear weapons as a deterrent.59 If the nuclear threshold is breached in a conflict between the United States and China, the risk of nuclear exchange is real. In short, if a coming revolution in military affairs provides a real or perceived battlefield advantage for Russia or China, such a development raises the likelihood of armed aggression against US regional allies, major power war, and an increased risk of nuclear escalation. implications Future scholarship should incorporate geopolitical conditions and the related foreign policy goals of the states in question when theorizing the effects of technology on international politics. Often scholars attempt to conceptualize the effects of weapons systems in isolation from the political context in which they are embedded. Studies treat technology as disembodied from geopolitics and as exerting independent effects on the international system. But technology does not float freely. Technology is a tool different actors can use in different ways. Bakers and arsonists employ fire in their crafts to strikingly different ends. In the current international environment, Russia and China would tend to employ technology toward advancing revisionist aims. Technological advances in these countries are therefore much more likely to disrupt the prevailing international order and nuclear strategic stability. This approach also suggests the potential threat new technology poses to nuclear strategic stability is more pervasive than previously understood. To undermine strategic stability, new technology need not directly impact strategic capabilities. Rather, any technology that promises to shift the local balance of power in Eastern Europe or the Indo-Pacific has the potential to threaten nuclear strategic stability. This understanding of this issue leads to different policy prescriptions. If the technology itself is the problem, then it must be controlled and should not be allowed to spread to any states. In contrast, the framework outlined here suggests a different recommendation: preserve the prevailing balance of power in Europe and Asia. Technological change that, on balance, reinforces the prevailing international system should strengthen stability. Leading democracies therefore, should increase investments in emerging technology to maintain a technological edge over their adversaries. Export control and nonproliferation measures should be designed to deny emerging military technology to Russia and China. Arms control should be negotiated with the primary objective of sustaining the current international distribution of power. Making progress in these areas will be difficult. But the consequences of failure could be shifts in the international balance of power, conflict among great powers, and an increased risk of nuclear war.

The impact is human extinction.

Clare 25 [Stephen Clare (former research fellow @ the Forethought Foundation) 03-xx-2025, "Great power war", 80,000 Hours, https://80000hours.org/problem-profiles/great-power-conflict/, accessed 08-12-25]

A modern great power war could see nuclear weapons, bioweapons, autonomous weapons, and other destructive new technologies deployed on an unprecedented scale.¶ It would probably be the most destructive event in history, shattering our world. It could even threaten us with extinction.¶ We've come perilously close to just this kind of catastrophe before.¶ On October 27, 1962 — near the peak of the Cuban Missile Crisis — an American U-2 reconnaissance plane set out on a routine mission to the Arctic to collect data on Soviet nuclear tests. But, while flying near the North Pole, with the stars obscured by the northern lights, the pilot made a navigation error and strayed into Soviet airspace.1¶ Soviet commanders sent fighter jets to intercept the American plane. The jets were picked up by American radar operators and nuclear-armed F-102 fighters took off to protect the U-2.¶ Fortunately, the reconnaissance pilot realised his error with enough time to correct course before the Soviet and American fighters met. But the intrusion enraged Soviet Premier Nikita Khrushchev, who was already on high alert amidst the crisis in Cuba.¶ "What is this, a provocation?" Khrushchev wrote to US President John F. Kennedy. "One of your planes violates our frontier during this anxious time when everything has been put into combat readiness."¶ If the U-2's path had strayed further west, or the Soviet fighters had been fast enough to intercept it, this incident could have played out quite differently. Both the United States and the USSR had thousands of nuclear missiles ready to fire. Instead of a nearly-forgotten anecdote, the U-2 incident could have been a trigger for war, like the assassination of Franz Ferdinand.¶ Competition among the world's most powerful countries shapes our world today. And whether it's through future incidents like the lost U-2, or something else entirely, it's plausible that it could escalate and lead to a major, devastating war.¶ Is there anything you can do to help avoid such a terrible outcome? It is, of course, difficult to imagine how any one individual can hope to influence such world-historical events. Even the most powerful world leaders often fail to predict the global consequences of their decisions.¶ But I think the likelihood and severity of great power war makes this among the most pressing problems of our time — and that some solutions could be impactful enough that working on them may be one of the highest-impact things to do with your career.¶ By taking action, I think we can create a future where the threat of great power war is a distant memory rather than an ever-present danger.¶ Summary¶ Economic growth and technological progress have bolstered the arsenals of the world's most powerful countries. That means the next war between them could be far worse than World War II, the deadliest conflict humanity has yet experienced.¶ Could such a war actually occur? We can't rule out the possibility. Technical accidents or diplomatic misunderstandings could spark a conflict that quickly escalates. Or international tension could cause leaders to decide they're better off fighting than negotiating.¶ It seems hard to make progress on this problem. It's also less neglected than some of the problems that we think are most pressing. There are certain issues, like making nuclear weapons or military artificial intelligence systems safer, which seem promising — although it may be more impactful to work on reducing risks from AI, bioweapons or nuclear weapons directly. You might also be able to reduce the chances of misunderstandings and miscalculations by developing expertise in one of the most important bilateral relationships (such as that between the United States and China). ¶ Finally, by making conflict less likely, reducing competitive pressures on the development of dangerous technology, and improving international cooperation, you might be helping to reduce other risks, like the chance of future pandemics. ¶ Our overall view ¶ Recommended ¶ Working on this issue seems to be among the best ways of improving the long-term future we know of, but all else equal, we think it's less pressing than our highest priority areas (primarily because it seems less neglected and harder to solve). ¶ Scale ¶ There's a significant chance that a new great power war occurs this century. ¶ Although the world's most powerful countries haven't fought directly since World War II, war has been a constant throughout human history. There have been numerous close calls, and several issues could cause diplomatic disputes in the years to come. ¶ These considerations, along with forecasts and statistical models, lead me to think there's about a one-in-three chance that a new great power war breaks out in roughly the next 30 years. ¶ Few wars cause more than a million casualties and the next great power war would probably be smaller than that. However, there's some chance it could escalate massively. Today the great powers have much larger economies, more powerful weapons, and bigger military budgets than they did in the past. An all-out war could kill far more people than even World War II, the worst war we've yet experienced. ¶ Could it become an existentially threatening war — one that could cause human extinction or significantly damage the prospects of the long-term future? It's very difficult to say. But my best current guess is that the chance of an existential catastrophe due to war in

the next century is somewhere between 0.05% and 2%. ¶ Neglectedness ¶ War is a lot less neglected than some of our other top problems. There are thousands of people in governments, think tanks, and universities already working on this problem. But some solutions or approaches remain neglected. One particularly promising approach is to develop expertise at the intersection of international conflict and another of our top problems. Experts who understand both geopolitical dynamics and risks from advanced artificial intelligence, for example, are sorely needed. ¶ Solvability ¶ Reducing the risk of great power war seems very difficult. But there are specific technical problems that can be solved to make weapons systems safer or less likely to trigger catastrophic outcomes. And in the best case, working on this problem can have a leverage effect, making the development of several dangerous technologies safer by improving international cooperation and making them less likely to be deployed in war. ¶ At the end of this profile, I suggest five issues which I'd be particularly excited to see people work on. These are: ¶ Developing expertise in the riskiest bilateral relationships ¶ Learning how to manage international crises quickly and effectively and ensuring the systems to do so are properly maintained ¶ Doing research to improve particularly important foreign policies, like strategies for sanctions and deterrence ¶ Improving how nuclear weapons and other weapons of mass destruction are governed at the international level ¶ Improving how such weapons are controlled at the national level ¶ ¶ Why might preventing great power war be an especially pressing problem? ¶ A modern great power war — an all-out conflict between the world's most powerful countries — could be the worst thing to ever happen to humanity. ¶ Historically, such wars have been exceptionally destructive. Sixty-six million people died in World War II, likely the deadliest catastrophe humanity has experienced so far. ¶ Since World War II, the global population and world economy have continued to grow, nuclear weapons have proliferated, and military technology has continued to advance. This means the next world war could be even worse, just as World War II was much deadlier than World War I. ¶ It's not guaranteed that such a war will break out. And if it does, it may not escalate to such a terrible extent. But the chance can't be ignored. In fact, there are reasons to think that the odds of World War III breaking out this century are worryingly high. ¶ A modern great power war would be devastating for people alive today. But its effects could also persist long into the future. That's because there is a substantial chance that this century proves to be particularly important. Technologies with the potential to cause a global catastrophe or radically reshape society are likely to be invented. How we choose to develop and deploy them could impact huge numbers of our descendants. And these choices would be affected by the outcomes of a major war. ¶ To be more specific, there are three main ways great power conflict could affect the long-term future. ¶ High international tension could increase other risks. Great power tensions could make the world more dangerous even if they don't lead to war. During the Cold War, for example, the United States and the USSR never came into direct conflict but invested in bioweapons research and built up nuclear arsenals. This dynamic could return, with tension between great powers fueling races to develop and build new weapons, raising the risk of a disaster even before shots are fired. ¶ War could cause an existential catastrophe. If war does break out, it could escalate dramatically, with modern weapons (nuclear weapons, bioweapons, autonomous weapons, or other future technologies) deployed at unprecedented scale. The resulting destruction could irreparably damage humanity's prospects. ¶ War could reshape international institutions and power balances. While such a catastrophic war is possible, it seems extremely unlikely. But even a less deadly war, such as another conflict on the scale of World War II, could have very long-lasting effects. For example, it could reshape international institutions and the global balance of power. In a pivotal century, different institutional arrangements and geopolitical balances could cause humanity to follow different long-term trajectories. ¶ The rest of this profile explores exactly how pressing a problem great power conflict is. In summary: ¶ Great power relations have become more tense. (More.) ¶ Partly as a result, a war is more likely than you might think. It's reasonable to put the probability of such a conflict in the coming decades somewhere between 10% and 50%. (More.) ¶ If war breaks out, it would probably be hard to control escalation. The chance that it would become large enough to be an existential risk cannot be dismissed. (More.) ¶ This makes great power war one of the biggest threats our species currently faces. (More.) ¶ It seems hard to make progress on solving such a difficult problem (more) — but there are many things you can try if you want to help (more). ¶ International tension has risen and makes other problems worse ¶ Imagine we had a thermometer-like device which, instead of measuring temperature, measured the level of international tension.2 This 'tension metre' would max out during periods of all-out global war, like World War II. And it would be relatively low when the great powers3 were peaceful and cooperative. For much of the post-Napoleonic 1800s, for example, the powerful European nations instituted the Concert of Europe and mostly upheld a continental peace. The years following the fall of the USSR also seem like a time of relative calm, when the tension metre would have been quite low.4 ¶ How much more worried would you be about the coming decades if you knew the tension metre would be very high than if you knew it would be low? Probably quite a lot. In the worst case, of course, the great powers could come into direct conflict. But even if it doesn't lead to war, a high level of tension between great powers could accelerate the development of new strategic technologies, make it harder to solve global problems like climate change, and undermine international institutions. ¶ During the Cold War, for instance, the United States and USSR avoided coming into direct conflict. But the tension metre would still have been pretty high. This led to some dangerous events: ¶ A nuclear arms race. The number of nuclear warheads in the world grew from just 300 in 1950 to over 64,000 in 1986. ¶ The development of new bioweapons. Despite signing the Biological Weapons Convention in 1972, the search for military advantages motivated Soviet decision makers to continue investing in bioweapon development for decades. Although never used in combat, biological agents were accidentally released from research facilities, resulting in dozens of deaths and threatening to cause a pandemic.5 ¶ Nuclear close calls. Military accidents and false alarms happened regularly, and top decision makers were more likely to interpret these events hostilely when tensions were high. On several occasions it seems the decision about whether or not to start a nuclear war came down to individuals acting under stress and with limited time. ¶ This makes international tension an existential risk factor. It's connected to a number of other problems, which means reducing the level of international tension would lower the total amount of existential risk we face. ¶ The level of tension today ¶ Recently, international tension seems to have once again been rising. To highlight some of the most salient examples: ¶ China-United States relations have deteriorated, leading to harsh diplomatic rhetoric and protectionist trade policies that aim to reduce the countries' economic interdependence. ¶ Russia's invasion of Ukraine has killed about a hundred thousand people so far, raised the risk of nuclear war, and sent United States-Russia relations to their lowest point since the Cold War. ¶ Chinese and Indian soldiers fought deadly skirmishes along their countries' disputed border in 2020–21. ¶ These dynamics raise an important question: how much more dangerous is the world given this higher tension than it would be in a world of low tension? ¶ I think the answer is quite a bit more dangerous — for several reasons. First, international tension seems likely to make technological progress more dangerous. There's a good chance that, in the coming decades, humanity will make some major technological breakthroughs. We've discussed, for example, why one might worry about the effects of advanced artificial intelligence systems or biotechnology. The level of tension could strongly affect how these technologies are developed and governed. Tense relations could, for example, cause countries to neglect safety concerns in order to develop technology faster.6 ¶ Second, great power relations will strongly influence how nations do, or do not, cooperate to solve other global collective action problems. For example, in 2022, China withdrew from bilateral negotiations with the United States over climate action in protest of what it perceived as American diplomatic aggression in Taiwan. That same year, efforts to strengthen the Biological Weapons Convention were reportedly hampered by the Russian delegation after their country's invasion of Ukraine raised tensions with the United States and other western countries. ¶ And third, if relations deteriorate severely, the great powers could fight a war. ¶ How likely is a war? ¶ Wars are destructive and risky for all countries involved. Modern weapons, especially nuclear warheads, make starting a great power war today seem like a suicidal undertaking. ¶ But factors like the prevalence of war throughout history, the chance that leaders make mistakes, conflicting ideologies, and commitment problems, make me think that conflict could break out anyway. ¶ On balance, I think such an event is somewhat unlikely but hardly unthinkable. To quantify this: I put the chance we experience some kind of war between great powers before 2050 at about one-in-three.7 ¶ War has occurred regularly in the past. ¶ One reason to think a war is quite likely is that such conflicts have been so common in the past. Over the past 500 years, about two great power wars have occurred per century.8 ¶ Naively, this would mean that every year there's a 2% chance such a war occurs, implying the chance of experiencing at least one great power war over the next 80 years — roughly until the end of the century — is about 80%.9 ¶ This is a very simple model. In reality, the risk is not constant over time and independent across years. But it shows that if past trends simply continue, the outcome is likely to be very bad. ¶ Has great power war become less likely? ¶ One of the most important criticisms of this model is that it assumes the risk is constant over time. Some researchers have argued instead that, especially since the end of World War II, major conflicts have become much less likely due to: ¶ Nuclear deterrence: Nuclear weapons are so powerful and destructive that it's just too costly for nuclear-armed countries to start wars against each other.10 ¶ Democratisation: Democracies have almost never gone to war against each other, perhaps because democracies are more interconnected and their leaders are under more public pressure to peacefully resolve disputes with each other.11 The proportion of countries that are democratic has increased from under 10% in 1945 to about 50% today. ¶ Strong economic growth and global trade: Global economic growth accelerated following World War II and the value of global exports grew by a factor of almost 30 between 1950 and 2014. Since war disrupts economies and international trade, strong growth raises the costs of fighting.12 ¶ The spread of international institutions: Multilateral bodies like the United Nations General Assembly and Security Council promote diplomatic dialogue and facilitate coordination to punish transgressors.13 ¶ It is true that we are living through an unusually long period of great power peace. It's been about 80 years since World War II. We just saw that a simple model using the historical frequency of great power wars suggests there was only a 20% chance of going that long without at least one more war breaking out. This is some evidence in favour of the idea that wars have become significantly less common. ¶ ¶ At the same time, we shouldn't feel too optimistic. ¶ The numerous close calls during the Cold War suggest we were somewhat lucky to avoid a major war in that time. And a 20% chance of observing 80 years of peace is not that low.14 Structural changes might have dramatically reduced the likelihood of war. Or perhaps we've just been lucky. It could even be that technological advances have made war less likely to break out, but more deadly when it occurs, leaving the overall effect on the level of risk ambiguous. It just hasn't been long enough to support a decisive view.15 ¶ So while the recent historical trend is somewhat encouraging, we don't have nearly enough data to be confident that great power war is a thing of the past. To better predict the likelihood of future conflict, we should also consider distinctive features of our modern world.16 ¶ One might think that a modern great power war would simply be so destructive that no state leader would ever choose to start one. And some researchers do think that the destruction such a war would wreak globally makes it less likely to occur. But it would be hard to find anyone who claims this dynamic has driven the risk to zero. ¶ First, a war could be started by accident. ¶ Second, sometimes even prudent leaders may struggle to avoid a slide towards war. ¶ We could blunder into war. ¶ An accidental war can occur if one side mistakes some event as an aggressive action by an adversary. ¶ This happened several times during the Cold War. The earlier example of the wayward American reconnaissance plane shows how routine military exercises carry some escalation risk. Similarly, throughout history, nervous pilots and captains have caused serious incidents by attacking civilian planes and ships.17 Nuclear weapons allow for massive retaliatory strikes to be launched quickly — potentially too quickly to allow for such situations to be explained and de-escalated. ¶ It is perhaps more likely, though, that an accidental war could be triggered by a technological malfunction. Faulty computers and satellites have previously triggered nuclear close calls. As monitoring systems have become more reliable, the rate at which such accidents have occurred has been going down. But it would be overconfident to think that technological malfunctions have become impossible. ¶ Future technological changes will likely raise new challenges for nuclear weapon control. There may be pressure to integrate artificial intelligence systems into nuclear command and control to allow for faster data processing and decision making. And AI systems are known to behave unexpectedly when deployed in new environments.18 ¶ New technologies will also create new accident risks of their own, even if they're not connected to nuclear weapon systems. Although these risks are hard to predict, they seem significant. I'll say more about how such technologies — including AI, nuclear, biological, and autonomous weapons — are likely to increase war risks later. ¶ Leaders could choose war. ¶ All that said, most wars have not started by accident. If another great power war does break out in the coming decades, it is more likely to be an intentional decision made by a national leader. ¶ Explaining why someone might make such a costly, destructive, unpredictable, and risky decision has been called "the central puzzle about war." It has motivated researchers to search for "rationalist" explanations for war. In his 2022 book Why We Fight, for example, economist Chris Blattman proposes five basic explanations: unchecked interests, intangible incentives, uncertainty, commitment problems, and misperceptions.19 ¶ This section discusses how great power tensions may escalate to war in the next few decades. It focuses on three potential conflicts in particular: war between the US and China, between the US and Russia, and between China and India. These are discussed because each of these countries are among the world's largest economies and military spenders, and seem particularly likely to fight. At the end, I briefly touch on other potential large conflicts. ¶ United States-China ¶ The most worrying possibility is war between the United States and China. They are easily the world's largest economies. They spend by far the most on their militaries. Their diplomatic relations are tense and have recently worsened. And their relationship has several of the characteristics that Blattman identifies as causes of war. ¶ At the core of the United States-China relationship is a commitment problem. ¶ China's economy is growing faster than the United States'. By some metrics, it is already larger.20 If its differential growth continues, the gap will continue to widen between it and the United States. While economic power is not the sole determinant of military power, it is a key factor.21 ¶ The United States and China may be able to strike a fair deal today. But as China continues to grow faster, that deal may come to seem unbalanced. Historically, such commitment problems seem to have made these kinds of transition periods particularly dangerous.22 ¶ In practice, the United States and China may find it hard to agree on rules to guide their interactions, such as how to run international institutions or govern areas of the world where their interests overlap. ¶ The most obvious issue which could tip the United States-China relationship from tension into war is a conflict over Taiwan. Taiwan's location and technology industries are valuable for both great powers. ¶ This issue is further complicated by intangible incentives. ¶ For the United States, it is also a conflict over democratic ideals and the United States' reputation for defending its allies. ¶ For China, it is also a conflict about territorial integrity and addressing what are seen as past injustices. ¶ Still, forecasts suggest that while a conflict is certainly possible, it is far from inevitable. As of 8 June 2023, one aggregated forecast23 gives a 17% chance of a United States-China war breaking out before 2035.24 ¶ A related aggregated forecast of the chance that at least 100 deaths occur in conflict between China and Taiwan by 2050 gives it, as of 8 June 2023, a much higher 68% chance of occurring.25 ¶ United States-Russia ¶ Russia is the United States' other major geopolitical rival. ¶ Unlike China, Russia is not a rival in economic terms: even after adjusting for purchasing power, its economy is only about one-fifth the size of the United States'. ¶ However, Russia devotes a substantial fraction of its economy to its military. Crucially, it has the world's largest nuclear arsenal. And Russian leadership has shown a willingness to project power beyond their country's borders. ¶ ¶ Top five countries by estimated military spending, 2021. Source: SIPRI ¶ Russia's 2022 invasion of Ukraine demonstrated the dangers of renewed rivalry between Russia and the United States-led West. The war has already been hugely destructive: the largest war in Europe since World War II, with hundreds of thousands of casualties already and no end to the conflict in sight. And it could get much worse. Most notably, Russian officials have repeatedly refused to rule out the use of nuclear weapons. ¶ Unchecked interests and intangible incentives are again at play here. Vladimir Putin leads a highly-centralised government. He has spoken about how his desire to rebuild Russia's reputation played in his decision to invade Ukraine. ¶ Given their ideological differences and history of rivalry, it is reasonable to expect that the United States and Russia will continue to experience dangerous disagreements in the future. As of 8 June 2023, an aggregated forecast gives a 20% chance that the United States and Russia will fight a war involving at least 1,000 battle deaths before 2050. ¶ China-India ¶ India is already the world's third-largest economy. If national growth rates remain roughly constant, the size of the Indian economy will surpass that of the United States' sometime this century. India also has nuclear weapons and is already the world's third-largest military spender (albeit at a much lower level than China or the United States). ¶ One reason to worry that China and India could fight a war is that they already dispute territory along their border. Countries that share a border, especially when it is disputed, are more likely to go to war than countries that do not. By one count, 88% of the wars that occurred between 1816 and 1980 began as wars between neighbours.26 ¶ In fact, China and India already fought a brief but violent border war in 1962. Deadly skirmishes have continued since, resulting in deaths as recently as 2020. ¶ Forecasters agree that a China-India conflict seems relatively (though not absolutely) likely. An aggregated forecast gives a 19% chance of war before 2035. ¶ Other dangerous conflicts ¶ These three conflicts — United States-China, United States-Russia, and China-India — are not the only possible great power wars that could occur. Other potential conflicts could also pose existential risk, either because they drive dangerous arms races or see widespread deployment of dangerous weapons. ¶ We should keep in mind India-Pakistan as a particularly likely conflict between nuclear-armed states and China-Russia as a potential, though unlikely, conflict between great powers with a disputed border and history of war. Plus, new great powers may emerge or current great powers may fade in the years to come. ¶ While I think we should prioritise the three potential conflicts I've highlighted above, the future is highly uncertain. We should monitor geopolitical changes and be open to changing our priorities in the future. ¶ Overall predictions ¶ Below is a table listing relevant predictions from the forecasting platform Metaculus, including the number of predictions made, as of 10 March 2023. Note the different timescales and resolution criteria for each question; they may not be intuitively comparable. ¶ ¶ I have previously independently estimated the likelihood of seeing a World War II-like conflict this century. My calculation first adjusts historical base rates to allow for the possibility that major wars have become somewhat less likely, and uses the adjusted base rate to calculate the probability of seeing a war between now and 2100. ¶ This method gives a 45% chance of seeing a major great power war in the next 77 years. If the probability is constant over time then the cumulative probability between now and 2050 would be 22%. This is aligned with the Metaculus predictions above. ¶ We can also ask experts what they think. Unfortunately, there are surprisingly few expert predictions about the likelihood of major conflict. One survey was conducted by the Project for the Study of the 21st Century. The numbers were relatively aligned with the Metaculus forecasts, though slightly more pessimistic. However, it seems a mistake to put too much stock in this survey (see footnote).27 ¶ We now have at least a rough sense of a great power war's probability. But how bad could it get if it occurred? ¶ A new great power war could be devastating. ¶ At the time, the mechanised slaughter of World War I was a shocking step-change in the potential severity of warfare. But its severity was surpassed just 20 years later by the outbreak of World War II, which killed more than twice as many people. ¶ A modern great power war could be even worse. ¶ How bad have wars been in the past? ¶ The graph below shows how common wars of various sizes are, according to the Correlates of War's Interstate War dataset.28 ¶ The x-axis here represents war size in terms of the logarithm of the number of battle deaths. The y-axis represents the logarithm of the proportion of wars in the dataset that are at least that large. ¶ Using logarithms means that each step to the right in the graph represents a war not one unit larger, but 10 times larger. And each step up represents a war that is not one unit more likely, but 10 times more likely. ¶ What the graph shows is that wars have a heavy tail. Most wars remain relatively small. But a few escalate greatly and become much worse than average. ¶ Of the 95 wars in the latest version of the database, the median battle death count is 8,000. But the heavy tail means the average is 334,000 battle deaths. And the worst war, World War II, had almost 17 million battle deaths.30 ¶ The number of battle deaths is only one way to measure the badness of wars. We could also consider the proportion of the population of the countries involved who were killed in battle. By this measure, the worst war since 1816 was not World War II. Instead, it's the Paraguayan War of 1864–70. In that war, 30 soldiers died for every 1,000 citizens of the countries involved. It's even worse if we also consider civilian deaths; while estimates are very uncertain, it's plausible that about half of the men in Paraguay, or around a quarter of the entire population, was killed.31 ¶ What if instead we compared wars by the proportion of the global population killed? World War II is again the worst conflict since 1816 on this measure, having killed about 3% of the global population. Going further back in time, though, we can find worse wars. Ghengis Khan's conquests likely killed about 9.5% of people in the world at the time. ¶ The heavy tail means that some wars will be shockingly large.32 The scale of World War I and World War II took people by surprise, including the leaders who initiated it. ¶ It's also hard to know exactly how big wars could get. We haven't seen many really large wars. So while we know there's a heavy tail of potential outcomes, we don't know what that tail looks like. ¶ That said, there are a few reasons to think that wars much worse than World War II are possible. ¶ We're statistically unlikely to have brushed up against the end of the tail, even if the tail has an upper bound. ¶ Other wars have been deadlier on a per-capita basis. So unless wars involving countries with larger populations are systematically less intense, we should expect to see more intense wars involving as many people as World War II. ¶ Economic growth and technological progress are continually increasing humanity's war-making capacity. This means that, once a war has started, we're at greater risk of extremely bad outcomes than we were in the past. ¶ So how bad could it get?

How bad could a modern great power war be?

Over time, two related factors have greatly increased humanity's capacity to make war. 33 First, scientific progress has led to the invention of more powerful weapons and improved military efficiency. Second, economic growth has allowed states to build larger armies and arsenals. Since World War II, the world economy has grown by a factor of more than 10 in real terms; the number of nuclear weapons in the world has grown from basically none to more than 9,000, and we've invented drones, missiles, satellites, and advanced planes, ships, and submarines. Ghengis Khan's conquests killed about 10% of the world, but this took place over the course of two decades. Today that proportion may be killed in a matter of hours. First, nuclear weapons could be used. Today there are around 10,000 nuclear warheads globally.34 At the peak of nuclear competition between the United States and the USSR, though, there were 64,000. If arms control agreements break down and competition resurges among two or even three great powers, nuclear arsenals could expand. In fact, China's arsenal is very likely to grow — though by how much remains uncertain. Many of the nuclear weapons in the arsenals of the great powers today are at least 10 times more powerful than the atomic bombs used in World War II.35

Should these weapons be used, the consequences would be catastrophic. By any measure, such a war would be by far the most destructive, dangerous event in human history, with the potential to cause billions of deaths. The probability that it would, on its own, lead to humanity's extinction or unrecoverable collapse, is contested. But there seems to be some possibility — whether through a famine caused by nuclear winter, or by reducing humanity's resilience enough that something else, like a catastrophic pandemic, would be far more likely to reach extinction-levels (read more in our problem profile on nuclear war). Nuclear weapons are complemented and amplified by a variety of other modern military technologies, including improved missiles, planes, submarines, and satellites. They are also not the only military technology with the potential to cause a global catastrophe — bioweapons, too, have the potential to cause massive harm through

accidents or unexpected effects. What's more, humanity's war-making capacity seems poised to further increase in the coming years due to technological advances and economic growth. Technological progress could make it cheaper and easier for more states to develop weapons of mass destruction. In some cases, political and economic barriers will remain significant. Nuclear weapons are very expensive to develop and there exists a strong international taboo against their proliferation. In other cases, though, the hurdles to developing extremely powerful weapons may prove lower. Improvements in biotechnology will probably make it cheaper to develop bioweapons. Such weapons may provide the deterrent effect of nuclear weapons at a much lower price. They also seem harder to monitor from abroad, making it more difficult to limit their proliferation. And they could spark a global biological catastrophe, like a major — possibly existentially catastrophic — pandemic. Artificial intelligence systems are also likely to become cheaper as well as more powerful. It is not hard to imagine important military implications of this technology. For example, AI systems could control large groups of lethal autonomous weapons (though the timeline on which such applications will be developed is unclear). They may increase the pace at which war is waged, enabling rapid escalation outside human control. And AI systems could speed up the development of other dangerous new technologies. Finally, we may have to deal with the invention of other weapons which we can't currently predict. The feasibility and danger of nuclear weapons was unclear to many military strategists and scientists until they were first tested. We could similarly experience the invention of destabilising new weapons in our lifetime. What these technologies have in common is the potential to quickly kill huge numbers of people: A nuclear war could kill tens of millions within hours, and many more in the following days and months. A runaway bioweapon could prove very difficult to stop. Future autonomous systems could act with lightning speed, even taking humans out of the decision-making loop entirely. Faster wars leave less time for humans to intervene, negotiate, and find a resolution that limits the damage. How likely is war to damage the long-run future? When a war begins, leaders often promise a quick, limited conflict. But escalation proves hard to predict ahead of time (perhaps because people are scope-insensitive, or because escalation depends on idiosyncratic decisions). This raises the possibility of enormous wars that threaten all of humanity.