Contention 1 is sanctions

Trump just sanctioned the ICC, Debusmann 25 finds

Bernd Debusmann Jr, 02/07/24 , "Trump's sanctions condemned by ICC and Court vows to continue 'providing justice'," No Publication, https://www.bbc.com/news/articles/cx2p19l24g2o, accessed 2-7-2025 //RR

Top criminal court condemns **US sanctions** on officials 4 hours ago Share Save Bernd Debusmann Jr BBC Ne ws, White House Amy Walker BBC News Getty Images Donald Trump in **the** Oval Office. Getty Images Trump previously sanctioned **ICC** officials during his first term in office in 2020 The International Criminal Court (ICC) has vowed to continue its judicial work after US President Donald Trump signed an order to impose sanctions on its staff. The ICC said it "stands firmly" by its personnel and the order seeks to harm its "independent and impartial" work. **Trump's order accuses it of "illegitimate and baseless** actions", after the ICC issued an arrest warrant for Israeli Prime Minister Benjamin Netanyahu over alleged war crimes in Gaza, which Israel denies. The ICC also issued a warrant for a Hamas commander. The ICC is a global court, although the US and Israel are not members, with the power to bring prosecutions for genocide, crimes against humanity and war crimes. In its statement, it said: "The ICC condemns the issuance by the US of an executive order seeking to impose sanctions on its officials and harm its independent and impartial judicial work." It added it stood by its personnel, pledging "to continue providing justice and hope to millions of innocent victims of atrocities across the world". In recent years, the court has issued arrest warrants for Russian President Vladimir Putin over alleged war crimes in Ukraine, Taliban leaders for "persecuting Afghan girls and women" and Myanmar's military leader for crimes against the Rohingya Muslims. More than 120 countries are members, including the UK and many European nations. International Criminal Court: What is the ICC and what does it do? Judges at the court have said there are "reasonable grounds" to suggest Netanyahu, his former defence minister Yoav Gallant, and Hamas' Mohammed Deif - who died last year - bear "criminal responsibility for alleged war crimes and crimes against humanity". But a White House memo circulated on Thursday accused the Hague-based ICC of creating a "shameful moral equivalency" between Hamas and Israel by issuing the warrants at the same time. Trump's executive order said the ICC's recent actions "set a dangerous precedent" that endangered Americans by exposing them to "harassment, abuse and possible arrest". The order adds it "threatens to infringe upon the sovereignty of the United States" and "undermines" the national security and foreign policy work of the US and allies. **The sanctions**, announced while Netanyahu was in the US, **place financial and visa restrictions on individuals** and their families **who assist in ICC investigations** of American citizens or allies. The move has been met with condemnation by many US allies, including the Netherlands and Germany. A spokesperson for Prime Minister Keir Starmer said the UK supported the independence of the ICC.

Sanctions are imminent in the future as well. Kersten 25

Mark Kersten [Assistant Professor in the Criminology and Criminal Justice Department at the University of the Fraser Valley in British Columbia, Canada, and a Senior Consultant at the Wayamo Foundation in Berlin, Germany], 2025-02-12, "It's all about control: U.S. sanctions against the International Criminal Court and navigating a path forward," Justice in Conflict, https://justiceinconflict.org/2025/02/12/its-all-about-control-u-s-sanction-on-the-international-criminal-court-and-navigating-a-path-forward/, Date Accessed: 2025-02-13T23:22:29.561Z //RX

For now, however, the White House has decided not to sanction the Court as a whole but rather focus on a list of individuals to be targeted. **As this moment, only one person, ICC Prosecutor Karim Khan, has been listed. If the U.S. continues to target only individual ICC officials, the sanctions will neither paralyze nor destroy the Court.** They may interfere with certain actions and will certainly be figured into decision-making. For example, will Khan be permitted to speak at the United Nations Security Council, which he does twice a year, or to attend the Assembly of States Parties of the ICC conference when it takes place at the UN in New York? Regardless of the answers to these questions, sanctions targeting individuals are manageable, especially if the European Union invokes its Blocking Statute to insulate sanctioned ICC staff and ensuring they can access financial and banking institutions. Nevertheless, this is not a time to be complacent. As I have explained before and unlike the last round of U.S. sanctions, **the White House has four years**

to hurt the Court. If ICC investigators, prosecutors and judges continue their work in contexts like Palestine unabated and undeterred by American bullying, then the **Trump administration can escalate**; the Trump regime has a lot of runway left to issue new sanctions, **target the ICC as a whole with punitive sanctions** and perhaps even tariff countries that support the institution. Nothing is beyond the pale for this government. Avoiding a cycle of escalation while maintaining the integrity and independence of the Court will be a delicate balancing act. In navigating American hostility, it is important for the ICC and its supporters to be clear-eyed about the source of Washington's antipathy towards the Court. The easy answer is that **U.S. lawmakers are seeking retribution over the ICC's decision to issue a warrant for Israeli Prime Minister Benjamin Netanyahu and the possibility that the Court may do likewise for American servicemembers.** That is undoubtedly part of the equation, but American reactions to ICC investigations in specific contexts are just a symptom of a deeper cause driving Washington's antipathy towards the Court: a lack of control over the institution.

US sanctions will destroy the court in the long term,

Gusiev 24 [Glib Gusiev, edited Esquire magazine, now editor-in-chief for Babel; Oksana Kovalenko; graduated from Kyiv National University in International Relations, bachelors in law; "The US is threatening to destroy the International Criminal Court, the only court that can prosecute presidents for the most serious crimes. Why? And what does this mean for Ukraine?" accessed January 9 2025 and published December 30 2024]// RR

British lawyer Philip Sands, who worked on the creation of the court, writes in his book *Lawless World* that the ICC ultimately came about because of a US mistake. This happened in 1998 at a special legal conference in Rome, where 148 countries were supposed to adopt the statute of the future court. In the last hour of the last day of the conference, the head of the American delegation called for a vote on the text of the statute. He hoped that most states would not vote, understanding that there was no unanimity — and there was none. The vote took place: only seven participating countries voted against the statute. The US voted against, along with China and Israel. Despite this, the ICC was created. President Bill Clinton signed the statute of the court, but the US never ratified it. There is an informal but firm opinion in diplomatic circles that a treaty that is not adopted by full consensus has no long-term prospects. The ceremony that launched the signing of the Rome Statute, July 18, 1998. After that, countries began to join the International Criminal Court. As early as January 2001, when George W. Bush came to power, his administration began a campaign against the ICC. After the September 11 attacks, the United States launched a "war on terror," and then-Defense Secretary Donald Rumsfeld said his concerns about the ICC were growing because the court might try to establish jurisdiction over American servicemen. In May 2002, the George W. Bush administration announced that it would "rescind" its signature on the Rome Statute. And within three months, Congress had passed the U.S. Servicemen Protection Act, which lawyers call the "Hague Invasion Act." This law allows the US president to "use all necessary and appropriate means" to release any US citizen "held or imprisoned by the ICC." It prohibits the US from cooperating with the ICC, including sharing any intelligence. Finally, it prohibits the participation of US troops in UN peacekeeping operations unless the ICC grants them full immunity from prosecution. Lawyer Philip Sands calls these actions a policy of double standards: criminal courts are good enough for citizens of all countries, but not for Americans. But **the worst relations between the US and the ICC were during the time of Donald Trump.** The then ICC prosecutor, Fatou Bensouda, asked for permission to investigate crimes committed in Afghanistan, including by American soldiers. **Trump criticized the ICC from the rostrum of the UN General Assembly, and his administration canceled Bensouda's visa** — although the investigation did not begin. Sanctions against Bensouda personally did not stop the court, the investigation nevertheless began in 2020, and already in June 2020 Trump imposed sanctions against the ICC in general. He did not have time to seriously harm the court, because his successor, Joe Biden, lifted these sanctions in the spring of 2021. Donald Trump criticized the ICC in a speech to the UN General Assembly in September 2018. **The new US Presidential Administration has many ways to disrupt the work of the ISS** In June 2024, when the ICC was only considering issuing arrest warrants for the Israeli prime minister and defense minister, Republican Congressman Charles Roy introduced the "Anti-Illegitimate Trial" bill — referring to the ICC. It would require the president to impose sanctions on any foreigner who helps the ICC investigate Israeli crimes: seize their property or money, revoke their visas. **The US sanctions against the court and its prosecutor will have devastating consequences. They will make it almost impossible for US citizens to participate in the work of the Court, which will significantly limit the number of experts and scholars who cooperate with the ICC. The sanctions could also affect the court's finances, which are maintained in US dollars. The court will not be able to use American software, including databases. In addition, the court will have to close its New York office, which provides its connection to the UN**. Richard Goldstone, former Chief Prosecutor of the International Tribunals for Yugoslavia and Rwanda The House of Representatives voted for the bill in June of this year. It was sent to the Senate in September. Babel's interlocutors are concerned that Republicans will pass it, since they now have a majority in the Senate. In addition, the US

Congress annually allocates funds for international programs, including the ICC, through the State Department budget. Also, in 2024, Congress authorized the US president to transfer intelligence information about Russian crimes to the International Criminal Court, if requested. In 2024, the United States allocated $6 million to the ICC's economic support fund, at least $5 million to the victims' support fund, and a separate $3 million contribution to the Special Criminal Court in the Central African Republic. In the 2025 budget proposal, Republicans have already banned such cooperation and have also stipulated that any payments to the ICC are now prohibited. The bill has already been passed by the House of Representatives and forwarded to the Senate. Finally, the US president can impose sanctions by executive order.

However, the Affirmative grants immunity; halting sanctions. Article 48 of the Rome Statute states

ICRC, IHL Treaties, "Rome State," No Publication, https://ihl-databases.icrc.org/en/ihl-treaties/icc-statute-1998/article-48?activeTab=default, Date Accessed: 2025-02-07T19:46:24.292Z //RX

Article 48 Privileges and immunities 1. **The Court shall enjoy in the territory of each State Party such privileges and immunities as are necessary for the fulfilment of its purposes. 2. The judges**, the **Prosecutor**, the Deputy Prosecutors **and** the **Registrar shall**, when engaged on or with respect to the business of the Court, **enjoy** the same privileges and **immunities as are accorded to heads of diplomatic missions** and shall, after the expiry of their terms of office, continue to be accorded immunity from legal process of every kind in respect of words spoken or written and acts performed by them in their official capacity. The Deputy Registrar, the staff of the Office of the Prosecutor and the staff of the Registry shall enjoy the privileges and immunities and facilities necessary for the performance of their functions, in accordance with the agreement on the privileges and immunities of the Court. Counsel, experts, witnesses or any other person required to be present at the seat of the Court shall be accorded such treatment as is necessary for the proper functioning of the Court, in accordance with the agreement on the privileges and immunities of the Court. The privileges and immunities of: (a) A judge or the Prosecutor may be waived by an absolute majority of the judges; (b) The Registrar may be waived by the Presidency; (c) The Deputy Prosecutors and staff of the Office of the Prosecutor may be waived by the Prosecutor; (d) The Deputy Registrar and staff of the Registry may be waived by the Registrar.

An ineffective court has prevented prosecution of Rwanda. Amnesty International 25'

Amnesty International, 1-19-2025, "DR Congo: Rwandan-backed armed group and Congolese army must stop using explosive weapons in densely populated areas," https://www.amnesty.org/en/latest/news/2025/01/dr-congo-rwandan-backed-armed-group-and-congolese-army-must-stop-using-explosive-weapons-in-densely-populated-areas/, accessed 2-7-2025 //RR

DR Congo: Rwandan-backed armed group and Congolese army must stop using explosive weapons in densely populated areas Inaccurate explosive weapons with wide area effects used in densely populated areas more than 150 times in a seven-month period, killing over 100 people. Amid fresh uptick in fighting, warring parties must immediately cease attacks on civilians and stop using explosive weapons with wide area effects in populated areas. The ICC should consider investigating these attacks as war crimes. Between January and July 2024, in eastern Democratic Republic of Congo (DRC), the Rwandan-backed M23 armed group and the Congolese army (FARDC) launched explosive weapons with wide area effects into densely populated areas more than 150 times. **These attacks**, which killed more than 100 civilians and wounded hundreds, **violated international** humanitarian **law and** likely **constitute war crimes**, Amnesty International said. Amnesty International interviewed 60 people, visited several strike sites and analysed dozens of verified photos, videos and statements from the warring parties and others. Amnesty documented the M23 and Congolese army repeatedly using ground-launched unguided rockets, including 122mm Grad rockets. **These weapons systems are inherently inaccurate and their use in populated areas poses an extremely high risk of civilian**

casualties. “The devastating escalation in the use of explosive weapons is a new and dangerous development in a three-decade conflict already rife with human rights and humanitarian law violations,” said Agnès Callamard, Secretary General of Amnesty International. “Amid a fresh uptick in fighting, the M23 and the Congolese army must stop firing rockets, mortars and other explosives with wide area effects into densely populated areas. The warring parties must comply with international humanitarian law by taking all feasible precautions to avoid or minimize civilian harm during attacks.” Bombings by both sides **Under international humanitarian law (IHL), parties to a conflict must always distinguish between combatants and civilians. IHL prohibits disproportionate or indiscriminate attacks and demands parties to a conflict take feasible precautions to avoid, and in any event, to minimize harm to civilians. Launching an indiscriminate attack which kills or injures civilians is a war crime**. When used in populated areas, explosive weapons with wide-area effects are very likely to have indiscriminate effects and cannot be narrowly directed at a specific military target as required by IHL. In recent armed conflicts, explosive weapons have been the main cause of suffering of the civilian population, routinely used in blatant disregard of the clear rules of international humanitarian law for the protection of civilians. This situation prompted 83 Member States to endorse in 2022 the Political Declaration on Strengthening the Protection of Civilians from the Humanitarian Consequences arising from the use of Explosive Weapons in Populated Areas.

A strong ICC is a necessity to stop the conflict. Mufuni 25 finds

Sammy Mufuni, 2-7-2025, "Rwanda-backed rebels launch new offensive in DR Congo," No Publication, https://www.thetimes.com/world/africa/article/drc-congo-rebels-m23-rwanda-pm2t0pzrv?region=global, accessed 2-7-2025 //RR

The United Nations has warned that **the risk of regional conflict in central Africa “has never been higher”,** as **a rebel group backed by troops and weapons from Rwanda** closed in on a second key city in eastern Congo. **The M23 group and its Rwandan allies seized the city of Goma** last week and on Friday were pushing into the neighbouring South Kivu province. **Thousands have died and huge numbers have been displaced as the combined force has overtaken swathes of mineral-rich territory in the Democratic Republic of Congo, routing its troops and allies in one of the bloodiest chapters of the unrest that has lasted for decades**. Paul Kagame, Rwanda’s president, and his Congolese counterpart Felix Tshisekedi are due to attend a summit in Tanzania on Saturday as regional powers try to defuse the crisis. Corneille Nangaa, the head of a rebel alliance that includes M23, told a crowd in Goma that the group wanted to “liberate all of the Congo”. Advertisement Volker Türk, the UN’s rights chief, warned that “the risk of violence escalating throughout the sub-region has never been higher”. The rebels were within striking distance of Bukavu, the capital of South Kivu, on Friday and Congolese forces were braced to defend Kavumu, one of the last towns in their path, 20 miles short of the city. **In Goma, where the M23 has already installed its own mayor and authorities, the group dragooned tens of thousands of people to a rally at the stadium, telling them their city had been “liberated and sanitised”. A child watches as workers in protective suits carry bodies in a cemetery in Goma, Democratic Republic of Congo.**

An unstopped war is devastating. Amnesty 24 finds

Amnesty , 10-29-2024, "Why is the Democratic Republic of Congo wracked by conflict?," Amnesty International, https://www.amnesty.org/en/latest/campaigns/2024/10/why-is-the-democratic-republic-of-congo-wracked-by-conflict/, accessed 2-7-2025 //MA

The conflicts in the DRC have ignited a human rights catastrophe. Thousands of civilians are caught in the crossfire and [redacted] violence is rampant. **War crimes and crimes against humanity have been documented. Those who survive the violence face mass displacement, hunger, disease and poverty.** Mass killings and injuries through attacks targeted at civilians and indiscriminate attacks Mass [redacted] and other sexual violence Torture, enforced disappearances and arbitrary detentions Mass displacement and lack of access to food and shelter Poverty and lack of access to healthcare and education Mass killings and

injuries Fighting between armed forces in the DRC is often characterized by targeted or indiscriminate attacks that result in mass killings and injuries. **More than 6 million people have died as a result of conflict in the DRC** since 1998, many of them killed by hunger and disease. Today, **civilians are being killed in intensified fighting across North Kivu province. Casualties include those living in sites for internally displaced persons, which are regularly the targets of bombings.**

And Unstable states cause great power wars. Grygiel 9 finds

Grygiel 9 – George H. W. Bush Associate Professor of International Relations at the Paul H. Nitze School of Advanced International Studies at the Johns Hopkins University (Jacob, "Vacuum Wars", The American Interest July 1, 2009) RMT

The prevailing view of failed states is, to repeat, not wrong, just incomplete—for it ignores the competitive nature of great power interactions. The traditional understanding of power vacuums is still very relevant. Sudan, Central Asia, Indonesia, parts of Latin America and many other areas are characterized by weak and often collapsing states that are increasingly arenas for great power competition. The interest of these great powers is not to rebuild the state or to engage in "nation-building" for humanitarian purposes but to establish a foothold in the region, to obtain favorable economic deals, especially in the energy sector, and to weaken the presence of other great powers. Let's look at just three possible future scenarios. In the first, imagine that parts of Indonesia become increasingly difficult to govern and are wracked by riots. Chinese minorities are attacked, while pirates prowl sealanes in ever greater numbers. Bejing, pressured by domestic opinion to help the Chinese diaspora, as well as by fears that its seaborne commerce will be interrupted, intervenes in the region. China's action is then perceived as a threat by Japan, which projects its own power into the region. The United States, India and others then intervene to protect their interests, as well. In the second scenario, imagine that Uzbekistan collapses after years of chronic mismanagement and continued Islamist agitation. Uzbekistan's natural resources and its strategic value as a route to the Caspian or Middle East are suddenly up for grabs, and Russia and China begin to compete for control over it, possibly followed by other states like Iran and Turkey. In a third scenario, imagine that the repressive government of Sudan loses the ability to maintain control over the state, and that chaos spreads from Darfur outward to Chad and other neighbors. Powers distant and nearby decide to extend their control over the threatened oil fields. China, though still at least a decade away from having serious power projection capabilities, already has men on the ground in Sudan protecting some of the fields and uses them to control the country's natural resources. These scenarios are not at all outlandish, as recent events have shown. Kosovo, which formally declared independence on February 17, 2008, continues to strain relationships between the United States and Europe, on the one hand, and Serbia and Russia, on the other. The resulting tension may degenerate into violence as Serbian nationalists and perhaps even the Serbian army intervene in Kosovo. It is conceivable then that Russia would support Belgrade, leading to a serious confrontation with the European Union and the United States. A similar conflict, pitting Russia against NATO or the United States alone, or some other alliance of European states, could develop in several post-Soviet regions, from Georgia to the Baltics. Last summer's war in Georgia, for instance, showed incipient signs of a great power confrontation between Russia and the United States over the fate of a weak state, further destabilized by a rash local leadership and aggressive meddling by Moscow. The future of Ukraine may follow a parallel pattern: Russian citizens (or, to be precise, ethnic Russians who are given passports by Moscow) may claim to be harassed by Ukrainian authorities, who are weak and divided. A refugee problem could then arise, giving Moscow a ready justification to intervene militarily. The question would then be whether NATO, or the United States, or some alliance of Poland and other states would feel the need and have the ability to prevent Ukraine from falling under Russian control. Another example could arise in Iraq. If the United States fails to stabilize the situation and withdraws, or even merely scales down its military presence too quickly, one outcome could be the collapse of the central government in Baghdad. The resulting vacuum would be filled by militias and other groups, who would engage in violent conflict for oil, political control and sectarian revenge. This tragic situation would be compounded if Iran and Saudi Arabia, the two regional powers with the most direct interests in the outcome, entered the fray more directly than they have so far. In sum, there are many more plausible scenarios in which **a failed state could become a playground of both regional and great power rivalry, which is why we urgently need to dust off the traditional view of failed states and consider its main features as well as its array of consequences. The traditional view starts from a widely shared assumption that, as nature abhors vacuums, so does the international system. As Richard Nixon once said to Mao Zedong, "In international relations there are no good choices. One thing is sure—we can leave no vacuums, because they can be filled."6 The power vacuums created by failed states attract the interests of great powers because they are an easy way to expand their spheres of influence while weakening their opponents or forestalling their intervention. A state that decides not to fill a power vacuum is** effectively inviting other states to do so, thereby potentially decreasing its own relative power. This simple, inescapable logic is based on the view that international relations are essentially a zero-sum game: My gain is your loss. A failed state creates a dramatic opportunity to gain something, whether natural resources, territory or a strategically pivotal location. The power that controls it first necessarily increases its own standing relative to other states. As Walter Lippmann wrote in 1915, the anarchy of the world is due to the backwardness of weak states; . . . the modern nations have lived in armed peace and collapsed into hideous warfare because in Asia, Africa, the Balkans, Central and South America there are rich territories in which weakness invites exploitation, in which inefficiency and corruption invite imperial expansion, in which the prizes are so great that the competition for them is to the knife.7 The threat posed by failed states, therefore, need not emanate mainly from within. After all, by definition a failed state is no longer an actor capable of conducting a foreign policy. It is a politically inert geographic area whose fate is dependent on the actions of others. The main menace to international security stems from competition between these "others." As Arnold Wolfers put it in 1951, because of the competitive nature of international relations, "expansion would be sure to take place wherever a power vacuum existed."8 The challenge is that the incentive to extend control over a vacuum or a failed state is similar for many states. In fact, even if one state has a stronger desire to control a power vacuum because of its geographic proximity, natural resources or strategic location, this very interest spurs other states to seek command over the same territory simply because doing so weakens that state. The ability to deprive a state of something that will give it a substantial advantage is itself a source of power. Hence a failed state suddenly becomes a strategic prize, because it either adds to one's own power or subtracts from another's

The draw-in causes extinction.

Clare 23 [Stephen Clare, former research fellow @ the Forethought Foundation, 6-xx-2023, Great power war, 80,000 Hours, https://80000hours.org/problem-profilesgreat-power-conflict/] //RR

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, we have 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.¶ How 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 or used.¶ 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 kind of 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 conflict humanity has experienced so far.¶ Since World War II, the global population has continued to grow, nuclear weapons have proliferated, and military technology has continued to advance. This means that 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 very 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've thought a few years ago. I 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 meter' 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.¶ 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.¶ Pakistan 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.¶ 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 plausibly possible, it is far from inevitable. As of 8 June 2022, 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 2030.¶ 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 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 prediction¶ 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 III-like conflict this century. My calculation first adjusts historical base rates to allow for the possibility that major wars have become somewhat more 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 prediction 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. Genghis 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, th**e 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.

Contention 2 is Cyber.

Trump pursuing aggressive cyber policy, Vikram 24'

Vikram '24 [Virpratap Vikram; Research Fellow, Cyber Power and Future Conflict Programme which explores global strategic competition and future warfare. Prior to joining the IISS, Virpratap was the Research and Program Coordinator for the Cyber Program at Columbia University's School of International and Public Affairs in New York City. As the Competition Director for the NYC Cyber 9/12 Strategy Challenge, co-hosted by the Atlantic Council and Columbia SIPA, he played a key role in designing and organising the cyber crisis competition, which engaged over a thousand students. He formerly worked as a consultant for the Atlantic Council, where he co-authored a report on maritime cybersecurity. A 2020 graduate of Columbia SIPA's Master of International Affairs programme, Virpratap previously managed publishing and content for Gateway House in Mumbai, where he anchored their flagship podcast series. Virpratap's work has been published by the NATO Cooperative Cyber Defence Centre of Excellence, the Council on Foreign Relations, the Atlantic Council, Observer Research Foundation India and OODA Loo; Anticipating Trump's influence on US Cyber Command, 12-13-2024; IISS, https://www.iiss.org/cyber-power-matrix/anticipating-trumps-influence-on-us-cyber-com mand/; accessed, 2-11-2025 //RR+MA+ST+VT+RX+AK+HL+AT+RA+TW+RW+PP+RS+EM+EK+CC

The new Trump administration is likely to adjust how the United States positions itself and engages with adversaries in cyberspace. Amidst a series of geopolitical crises, **the risk of escalation in cyberspace grows**. Donald **Trump's administration is expected to return with a 'peace through strength' foreign policy, in contrast to Joe Biden's emphasis on collaborative cyber diplomacy and expanding the federal government's role in regulating cyberspace. If past discourse is prologue, then the new administration's approach will focus on American power projection in cyberspace by doubling down on the United States Cyber**

Command's (USCYBERCOM) capacity to take action. These posture shifts are set to create conditions that may further destabilise cyberspace and potentially spill over into the physical domain. As the US faces multiple conflicts with Russia, North Korea, Iran and China, this change would redefine its cyber strategy, raising critical questions about the balance between offense and stability. Trump's first administration was characterised by aggressive posturing, implementing the doctrine of persistent engagement and relaxing operational restrictions to strengthen the United States' position in cyberspace. This approach – considered necessary – marked a significant departure from the Barack Obama administration which focused on building policy and spreading awareness to defend against cyber threats. Moving on offense During his first candidates' debate with Hillary Clinton on 27 September 2016, Trump said that cyber 'is a huge problem' and the US had to get tougher on 'cyber warfare'. This came weeks after the Obama administration struggled to respond to Russian election interference, in which Wikileaks published documents stolen from the Democratic National Convention. Critics believed the administration failed to deter adversaries and encouraged a perception of US weakness in cyberspace. In his first year, Trump approved a delayed Pentagon plan to elevate USCYBERCOM into a unified combatant command. This plan allowed USCYBERCOM to competitively petition for US Department of Defense (DoD) resources while also signalling a forward-leaning shift in US posturing around cyber capabilities. In April 2018, USCYBERCOM outlined its strategic vision with a doctrine of persistent engagement, framing cyberspace as a domain of constant contact with adversaries that required proactive action, including in allied networks. It would take time for policymakers to understand that persistent engagement had been operationalised as defend forward – another concept outlined in the 2018 DoD Cyber Strategy which involves disrupting operations at their point of origin, potentially within foreign networks, before they are used against US systems. In August 2018, Congress included notable provisions in the 2019 National Defense Authorization Act (NDAA) that allowed the Secretary of Defense to approve the conduct of 'clandestine military activity' in cyberspace to defend and protect the US. Days later, Trump signed National Security Presidential Memoranda 13 (NSPM13), which removed Obama-era restrictions on offensive cyber operations allowing USCYBERCOM more leeway to conduct operations without presidential approval. This shift gave USCYBERCOM the autonomy to act swiftly, often at the cost of diplomacy. Trump undertook a number of decisions to move military decisions out of the White House, including the removal of the national cyber security coordinator who managed policy on offensive cyber operations. USCYBERCOM significantly scaled up its operational load under NSPM13 and the provisions in the 2019 NDAA. This proactive stance allowed it to remain more aggressive in cyberspace, and maintain a persistent engagement with adversaries to deter potential cyber threats. In the lead-up to the 2018 mid-term elections, Trump authorised USCYBERCOM to shut down internet access for the Russian Internet Research Agency troll farm, effectively reducing interference efforts. The president was not informed about plans to target Russia's power grid with disruptive malware, an operation aimed at deterring the Kremlin's electoral interference and to signal persistence to the Russians by pre-positioning cyber capabilities on their critical infrastructure which could be activated in the event of conflict. Trump has also used cyber capabilities to de-escalate crises. In 2019, following the destruction of an unmanned US drone by Iran, Trump opted against a conventional strike and authorised a retaliatory cyber attack on Iranian rocket and missile battery systems. Pushing for action Throughout 2024, an active set of Chinese state-sponsored actors have continued to conduct pre-positioning activity on US critical infrastructure in preparation for potential conflict with the US. Unlike the US operation on Russia's power grids in 2018, the US has clarified to China that its broad-based targeting behaviour is 'dangerous, escalatory, and it's not acceptable'. The incoming Trump administration has already been asked by Microsoft to 'push harder' to counter Russian and Chinese cyber activity. In a quest to demonstrate its seriousness on the issue, the administration could push for the creation of a US Cyber Force, akin to Trump's previous initiative to create the US Space Force. An internal study at USCYBERCOM is currently underway to assess the feasibility of such a force. Congress remained keen on an independent third-party study over DoD objections that a new military branch would be disruptive, yet the finalised 2025 NDAA removed the requirement of a cyber force study. This slows Congress's momentum on the issue and gives the Trump administration a greater role in the creation of a US Cyber Force. Amidst a period of immense geopolitical instability, USCYBERCOM deployed the Cyber National Mission Force 85 times in 30 countries in 2024, up from 50 deployments in 23 countries as of 2023. It is prepared to take more decisive action through enhanced authorities granted by the 2021 and the 2022 NDAA. These measures have eliminated USCYBERCOM's spending caps for programs and personnel and provided its commander with full budgetary and resource control for its missions and objectives. Weighing risks of escalation Efforts by China's Volt Typhoon and Salt Typhoon to pre-position capabilities and demonstrate persistence in US critical infrastructure are believed to be an effort to deter the US from countering Chinese influence in the Indo-Pacific and defending allies like Taiwan and the Philippines. Scholars have argued that cyber capabilities have limited effect in conflict and are poor tools of coercion. Yet, the last three decades have witnessed an escalation through the expansion in scope and scale of cyber operations against the US, and the global spread of cyber capabilities in foreign militaries. With China having demonstrated its persistent presence within US critical infrastructure, the Trump administration will have to weigh its responses based on the destabilising mechanisms that exist within cyberspace. The actions available to USCYBERCOM may also soon change as part of its evolving operational mandate. It has already moved to link its cyber operations with cyber-enabled information operations – which would better align it with other US allies. While the dual-hat relationship between USCYBERCOM and the National Security Agency has not been a central issue in the ongoing discussion on a US Cyber Force, the incoming Trump administration may revive its former plan to end the relationship. **As Trump assembles his second cabinet, he has chosen loyalty over all other concerns**. This raises questions in light of a June 2024 investigation of a Trump-era disinformation operation that targeted the Philippines to affect China's COVID-19 vaccine diplomacy. It also raises questions of whether provisions made in the 2019 and 2020 NDAA enabling the Secretary of Defense to order clandestine cyber and information operations might deviate from existing US doctrine and practices, and undermine international cyberspace norms. The risks of such destabilising behaviour are heavily dependent on who Trump appoints to key cyber policy positions and whether they can preserve a sense of continuity with the Biden administration's current efforts. Signalling adversaries The actions pursued by **Trump's new administration** will **alter** how adversaries **perceive** the US and, if it fails to deter them, might **spark their pursuit of additional cyber capabilities and encourage them to take bolder risks**. Similarly, **conditions for escalation** arise if the US establishment continues to remain unclear of its adversary's risk tolerance and considers that it has forgone the tacit agreements of peacetime. The Trump administration – like those before it – will now set the tone for how the US responds, dissuades and otherwise shapes state-driven activity in cyberspace, with far reaching global implications.

Aff solves as the ICC puts U.S. cyber attacks under jurisdiction. Wells '23,

[Jeffrey Wells, Partner at Sigma7, a risk services company, where he leads the Global Cyber Risk and Intelligence Practice, and is a George Mason University National Security Institute Visiting Fellow, "Uncrossed Wires — Cyberspace and Gavels: Navigating the ICC's New Mandate on Cyberwar Crimes," 11/20/2023, The SCIF, https://thescif.org/uncrossed-wires-cyberspace-and-gavels-navigating-the-iccs-new-mandate-on-cyberwar-crimes-23dbf410238 7, Accessed 02/06/2025] // MA

In a **significant step forward,theInternational Criminal Court (ICC) has expanded its purview to includespecific cyber-attacks under the umbrella of potential war crimes. This mainly concerns cyber-attackstargeted at essential services and facilities — like electricity networks, hospitals, and banks — that, if disrupted, could put civilian lives at risk or cause substantial harm. Such acts, by their nature, could breach the established rules of international conflict, drawing the scrutiny and potential action of the ICC. This move underscoresthe evolving landscape of warfare and the need to protect**

citizensin an increasingly digital world. Cyberoperations that target mobile communications andpower infrastructure, aiming to disrupt the enemy's communication, command, control, and intelligence — thereby shaping the battlefield for integrated military tactics — **could**also**be interpreted as war crimes**. By targeting cyber aggression, particularly against civilian infrastructure, the ICC looks to set a global standard for holding perpetrators accountable. Why it matters: The decision to prosecute cyberwar crimes under the framework of the ICC's Rome Statute and equate them with traditional forms of war crimes is an explicit acknowledgment of the severity and potential devastation these acts can inflict. The decision also underscores the urgent need for a concrete legal mechanism to deter and, when necessary, prosecute those who exploit the digital realm to commit acts of aggression against sovereign nations and their civilian populations. Future ICC judgments and other determinations may have significant implications for current US military doctrine and could reshape the landscape of international law and cyber warfare globally. Understanding the challenges and consequences of this expansion is essential. The debate: Attributing cyberattacks to specific actors is a persistent challenge due to the clandestine nature of cyber operations, the use of proxies, and advanced persistent threats. This attribution challenge can lead to legal uncertainty, diplomatic tensions, and the erosion of deterrence in cyberspace. **The ICC mandate may have unintended consequences for US** and NATO **cyber operations**, both those that occurred in the past and those **taking place in the future. These consequences could include retroactive accountability, increasing geopolitical tensions**, and reconsidering strategies and tactics in response to the evolving legal landscape. What's next: As the ICC broadens its scope to include cyberwar crimes, global collaboration is urgently needed to create effective strategies for this new era. Policymakers, military strategists, and legal experts must work together to develop a comprehensive framework that balances national security and accountability. Key steps should include: Developing a Standardized Protocol for International Cyber Incidents: Establishing guidelines for identifying the sources of cyberattacks, enabling diplomatic dialogues, and ensuring coordinated international responses. Establishing International Cyber Agreements: These should mirror arms control treaties, limit specific cyber capabilities, increase transparency, and provide dispute resolution mechanisms. Forming Cybersecurity Partnerships: The U.S. and other nations should establish bilateral and multilateral alliances focused on exchanging threat intelligence and best practices, strengthening cyber defenses, and fostering a more secure digital environment. Creating International Cyber Norms in Collaboration with the UN: This should set guidelines for responsible state behavior in cyberspace, promoting global stability and cooperation. The bottom line: The ICC's **expansion into cyberwar crimes is a significant step in addressing cyber threats under international law. However, it brings forth challenges in attribution, the lack of clear definitions, and potential unintended consequences** for U.S. and NATO cyber operations. Exploring the establishment of international cyber norms offers an alternative approach rooted in diplomacy, cooperation, and conflict prevention. Balancing accountability with international cooperation is paramount in addressing cyberwar crimes, and further research and policy development in this field is essential.

AND accepting Rome's nebulosity creates hesitancy to act, which is good.

Neale 20 [Agnieszka Jachec-Neale, Researcher and Lecturer at Exeter Law School, The Unintended Consequences of International Court Decisions, Lieber Institute, 11-19-2020, https://lieber.westpoint.edu/unintended-consequences-international-courts-decisions/, //RR]**LOAC = Law of Armed Conflict**

The consequences of re-interpretating LOAC notions, such as "attack," could be **far-reaching** from a legal and practical point of view. Developments like those discussed above risk further fragmentation in the material sense of LOAC and international criminal law. Such developments are also likely to **disrupt the fragile balance** between military needs and humanitarian considerations in armed conflict. If tribunals criminalize conduct not regulated by the same terms under LOAC, then **confusion can ensue as to the practical application of LOAC by military operators**. **This could inadvertently cause military operators to unduly restrain themselves in how they operate during armed conflict.** They may refrain from undertaking otherwise lawful actions because of a perceived risk of criminal sanction. The law must be clear in order for military operators to be able to undertake the full spectrum of military operations in the heat of battle without the uncertainty of criminal consequences. Moreover, the law must be clear for military operators to train their forces before battlefield deployment and for lawyers to give advice during conflict.¶ This trend of courts interpreting LOAC differently for international criminal law purposes leaves States to decide whether to accept international courts' conclusions, or to follow the traditional way LOAC has been interpreted. It may be that States are comfortable relying on international criminal courts to restate the law, elucidating its aspects, and even contributing to progressive development of new norms. However, if not, States should be more vocal about their objections to such findings and should reassert their international law-making role. Either way, States should not be indifferent. Indifference can easily be interpreted as acceptance of the ICC's findings and therefore affirmation of this pattern of judicial sanctioning of ever-expanding categories of war crimes.¶ Last but not least, international criminal tribunals must not only remain mindful of the vitality of upholding the principle of legality, but also of the reality of future armed conflicts. In these conflicts both the fighting participants and protected persons will bear the brunt of reinterpretation of the legal framework regulating such conflicts.

US OCO posture escalates and undermines norms. The aff is key for norm setting and a

defensive change.

Valeriano & Jensen ’19 [Brandon Valeriano and Benjamin Jensen; Valeriano was a senior fellow at the Cato Institute. He is also the Bren Chair of Military Innovation at the Marine Corps University and serves as senior adviser for the Cyber Solarium Commission; The Myth of the Cyber Offense: The Case for Restraint, 1-15-2019; Policy Analysis No. 862, https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint; accessed, 2-10-2025]// RR+MA+ST+VT+RX+AK+HL+AT+RA+TW+RW+PP+RS+EM+EK+CC+BB+AF+NMM+ZD+EE+RP

New policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the **rules of the game.** Cyberspace, to date, has been a domain of political warfare and coercive diplomacy, a world of spies developing long-term access and infrastructure for covert action, not soldiers planning limited-objective raids. Recent policy shifts appear to favor the **soldier** over the **spy**, thus creating a **new risk of offensive cyber events triggering inadvertent escalation between great powers**. Senior leaders throughout the federal government should consider a more prudent and restrained approach to cyber operations. Building on Sir Julian Corbett’s Principles of Maritime Strategy, one of the preeminent works in 20th century military theory, **we argue for a defensive posture consisting of limited cyber operations aimed at restraining rivals and avoiding escalation**.5 This approach counsels stepping back from preemption and focusing on sharing intelligence and hardening targets (that is, updating systems to repair existing vulnerabilities). The United States should **exercise restraint** and **avoid preemptive strikes** against great powers in cyberspace. Cyber Command’s New, More Aggressive Policy In April 2018, United States Cyber Command released a new vision statement calling for “persistent action”6 to maintain cyber superiority.7 The document echoed other major studies portraying the United States as ceding the digital high ground to adversaries. For example, a 2018 Defense Science Board study claimed the “the United States has fallen behind its competitors in the cyber domain, both conceptually and operationally.”8 Similarly, the Cyber Command vision statement **portrays other** great power**s** as increasingly capable of deploying sophisticated cyber actions against the United States. Major competitors, according to the statement, are using cyber operations to alter the long-term balance of power, short of military force.9 In using cyber operations to undermine American power, it claims these actors—especially strategic competitors such as Russia and China—are threatening not just the U.S. military but the entire global infrastructure and open exchange of information. In fact, according to General Paul M. Nakasone, commanding general of Cyber Command, “the environment we operate in today is truly one of great-power competition, and in these competitions, the locus of the struggle for power has shifted towards cyberspace.”10 In response to these threats, Cyber Command contends that the United States needs a more aggressive strategy. Cyber Command envisions a new era of persistent action that retains cyber superiority for the United States**.** Drawing on **military doctrine**, the document defines cyberspace superiority as “the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary.” In this view, the United States must command the digital commons to ensure other nonmilitary actors can access and use the new domain. Doing so requires persistence, defined as “the continuous ability to anticipate the adversary’s vulnerabilities, and formulate and execute cyberspace operations to contest adversary courses of action under determined conditions.”11 This approach increasingly sees preemption as the only viable path to security. U.S. cyber operations will “influence the calculation of our adversaries, deter aggression, and clarify the distinction between acceptable and unacceptable behavior in cyberspace,” and, as a result, “improve the security and stability of cyberspace.”12 Achieving this new stability through persistent action depends on “scaling to the magnitude of the threat, removing constraints on [U.S.] speed and agility, and maneuvering to counter adversaries and enhance national security.”13 In other words, the **U**nited **S**tates must go on the **offense** and preempt threats in the cyber domain as a means of ensuring stability. **Cyber Command emphasizes** a

constant state of competition beneath the threshold of armed conflict and underscores the need for faster responses to adversary attacks.

This parallels broader policy developments in the Trump administration. First, persistent action is linked to the concept of "contact" in the 2018 **National Defense Strategy.1**4 The new defense strategy, along with the 2018 National Security Strategy, envisions constant competition between great powers as the norm in the 21st century.15 Renewed great-power competition requires a global operating model comprised of four layers (contact, blunt, surge, and homeland) designed to help the United States "compete more effectively below the level of armed conflict; delay, degrade, or deny adversary aggression; surge war-winning forces and manage conflict escalation; and defend the U.S. homeland."16 In this model, cyberspace becomes another domain in which the United States must achieve command of the commons to guarantee the larger international order. Securing command of the commons in the face of increasing cyber operations by China and Russia requires a policy framework that accelerates cyber offense.

Offensive cyber operations entail missions "intended to project power in and through foreign cyberspace."17 In August 2018, Trump granted the military the initiative to launch **offensive cyber operations with what appears to be little interagency consultation or coordination.**18 **Cyberspace became a domain for soldiers, not just networks of spies.** The move represented a dramatic shift from the **restraints on cyber operations imposed by the Obama administration**. Obama's Presidential Policy Directive 20 originally specified the conduct and content of cyberspace operations. Secretly issued in October 2012 after Congress failed to provide guidance for cyber operations, the directive authorized offensive cyber operations under certain conditions and only after careful interagency vetting.19 All operations had to be consistent with American values and had to balance the effectiveness of operations with the risk to all targets, as determined by the president and the national security adviser.20 This policy framework required decisionmakers to ask

whether more conventional operations would be better suited for the target as well as the extent to which the operation might compromise other espionage and cyber operations. It also sought to ensure cyber effects were nonlethal and limited in magnitude: a clear attempt to avoid escalation. Similarly, the guidelines portrayed cyberspace as dynamic and boundless, increasing the risk that operations spill over to affect partner countries or impact American citizens.

In moving to the new framework, **the Trump administration appears to be changing the rules of the game in cyberspace**. North Korea, Iran, Russia, and China have long been exploiting the digital connectivity of our world for covert operations to gain a position of advantage. They have exhibited less restraint or concern for the consequences of militarizing cyberspace than the United States. Yet, **what the cyber hegemon** (the **U**nited **S**tates) does **defines** the **character** of **cyber op**eration**s much more** than these **secondary actors**.21 Despite increasingly sophisticated operations, **between 2000 and 2016 cyberspace was a domain defined by political warfare and covert signaling to control escalation more than it was an arena of decisive action.22 Taking a more offensive posture and preempting threats at their source,** an action implied by the Cyber Command Vision Statement, **has the potential to change the character of cyber operations, and through it, 21st century great-power competition.23** The Character of Cyber Operations, 2000–2016 Evaluating the policy debate about offensive cyber operations requires empirically describing prevailing patterns and trends associated with how rival states employ their capabilities. Just as it is perilous to describe all wars based on observations of crucial cases such as the First World War, it is similarly dangerous to assume that high-profile cases such as the Stuxnet operation, which degraded Iranian nuclear capabilities, accurately represent all cyber strategy. Rather, developing cyber policy options and supporting strategies should start with a clear understanding of how states use the digital domain to achieve a position of advantage in long-term competition. Between 2000 and 2016, there have been 272 documented cyber operations between rival states.24 These exchanges are best thought of as major operations involving a foreign policy impact. Each operation therefore might involve thousands, if not millions, of individual incidents as adversaries hijack computer networks to launch distributed denial of service attacks (DDoS) or use sustained spear-phishing campaigns to gain access to key systems. Like other forms of covert action, for every cyber operation we learn about, there are surely countless others we do not know about, as well as failed access attempts. Using the Dyadic Cyber Incident Dataset, we can categorize these operations based on three major tactics: disruption, espionage, and degradation.25 Cyber disruptions are low-cost, low-pain initiatives, such as DDoS attacks and website defacements, that harass a target to signal resolve and gain a temporary position of advantage.26 Cyber espionage reflects efforts to alter the balance of information in a way that enables coercion.27 Cyber degradations are higher-cost, higher-pain-inducing efforts that seek to degrade or destroy some aspect of the target's cyberspace networks, operations, or functions.28 As strategies for achieving a position of advantage, degradation attacks typically involve coercion or efforts to compel or deter an adversary.29 To date, cyber operations do not appear to produce concessions by themselves. Offense, whether disruption, espionage, or degradation, does not produce lasting results sufficient to change the behavior of a target state.30 Only 11 operations (4 percent) appear to have produced even a temporary political concession, with the majority associated with sustained, multiyear counterespionage operations by U.S. operatives usually targeting China or Russia.31 Furthermore, each of these operations involved not just cyber actions, but other instruments of national power, such as diplomatic negotiations, economic sanctions, and military threats.32 Under the Obama administration, these operations were calibrated to limit escalation risks and took place alongside a larger series of diplomatic maneuvers designed to manage great-power relationships. For example, the United States used an interagency response to Chinese hacking that included covert retaliation but also involved pursuing a 2015 agreement to limit cyber-enabled economic warfare.33 In response to Russian actions, the United States pursed a mix of sanctions, diplomatic maneuvers, and cyber actions. This strategy of combining active defense and coercive diplomacy, the use of positive and negative instruments of power to alter adversary behavior, was also on display in Buckshot Yankee, the code name given to the U.S. retaliation against a massive intrusion of Defense Department networks by Russia in 2008.34 Notably, many in the cybersecurity community view such activities as defensive counterstrikes designed to raise the costs of future adversary incursions into U.S. networks, rather than viewing them as preemptive offensive actions.35 Cyber operations rarely work in isolation, and when they do, they tend to involve very sophisticated capabilities that impose costs and risks on the attacker.36 Because such attacks can degrade or even destroy the target's networks and operations in the short term, they can also undermine espionage operations that rely on gathering information over the long term. Degradation attacks therefore make up the minority (14.76 percent) of documented operations between rival states. The majority of cyber operations were limited disruptions and espionage. It is thus not surprising that given the limited objectives of most cyber operations, to date rival states have tended to respond proportionally or not at all. Returning to the data, between 2000 and 2016, only 89 operations (32.72 percent) saw a retaliatory cyber response within one year. Of those, 54 (60.7 percent) were at a low-level response severity (e.g., website defacements, limited denial of service attacks, etc.). Table 1 in the appendix compares the severity scores for cyber operations between rival states between 2000 and 2016.37 When rival states do retaliate, the responses tend to be proportional: that is, they tend to match the severity of the initial attack.38 Low-level responses beget low-level counterresponses as states constantly engage in a limited manner consistent with the ebbs and flows of what famed Cold War nuclear theorist Herman Kahn called "subcrisis maneuvering."39 Rarely does a response include an increase in severity. Instead, we witness counterresponses of a similar or lower level than the original intrusion or a response outside the cyber domain (for example, economic sanctions or legal indictment of specific individuals). The engagement is persistent but managed, and often occurs beneath an escalatory threshold.40 As seen in Table 2 in the appendix, this behavior appears to apply equally to each possible cyber strategy: disruption, espionage, and degradation. Espionage saw little retaliatory escalation, while disruption and degradation both exhibited more low-level responses. Of the remaining 35 operations that prompted retaliation, 25 (71.4 percent) were related to U.S. active defense responses to repeated Russian and Chinese cyber operations. That is, the United States preferred to wait on adversary networks, develop intelligence, and retaliate with precise strikes designed to undermine specific threats. This strategy was not preemptive. Consistent with the idea of active defense, the strategy is best thought of as a counterattack that exploits rival network intrusions. Cyber operations also offer a means of signaling future escalation risk as well as a cross-domain release valve for crises. Rival states use cyber operations as a substitute for riskier military operations. Consider the standoff between Russia and Turkey in 2016. After a Turkish F-16 shot down a Russian Su-24 Fencer, a wave of DDoS attacks hit Turkish state-owned banks and government websites.41 Similarly, China is responding to U.S. tariffs and increased freedom of navigation operations—provocatively sailing U.S. warships in waters that China claims—with increased cyber activity targeting military networks.42 Russia is using a broad-front cyber campaign in response to Western sanctions, infiltrating targets ranging from the anti-doping agencies and sports federations to Westinghouse, which builds nuclear power plants, and the Hague-based Organization for the Prohibition of Chemical Weapons.43 Rather than escalate with conventional military operations, cyber operations offer rivals a way to respond to provocations without significantly increasing tensions in a crisis. Better to have a Russian DDoS attack temporarily shut down Turkish networks than for Russian long-range missiles to target Turkish military bases. The Myth of the Offense Contrary to observed patterns of limited disruption and espionage, Cyber Command sees cyberspace as a domain fraught with increasing risk, where great powers such as China and Russia will undermine American power. The only solution, from this perspective, is to go on the offense. Yet, the **benefits of an offensive posture**, especially in **cyberspace, are** mostly **illusory** to date**. Instead, the cyber domain tends to be optimized for defense and deception, not decisive offensive blows**. Not only is offense likely the **weaker form of competition in cyberspace,** it also **risks inadvertent escalation**. The fear, suspicion, and misperception that

characterize interstate rivalries exacerbate the **risk** of offensive action in cyberspace. Cyber Command's 2018 persistent-action strategy aims to "expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins."44 Put in simple terms, the best defense is a good offense: get on adversary networks and stop cyber operations targeting the United States before they occur. Under this strategy, offensive cyber operations will also be preemptive in that they are designed to "contest dangerous adversary activity before it impairs [U.S.] national power."45 To use another sports metaphor, come out swinging. Go on the offense first and establish escalation dominance (that is, demonstrating such superior capabilities over the target state that it can't afford to escalate in response).46 According to Cyber Command, preemptive strikes will "impose . . . strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks."47 Whether through punishment, risk, or denial strategies, offensive actions theoretically alter the target's behavior by increasing the expected costs of targeting U.S. interests.48 Offensive action, according to this thinking, deters future aggression by signaling resolve and establishing escalation dominance. Yet, there are well-established reasons to doubt that offensive options produce the intended results in cyberspace. Defense and Deception The rationale behind persistent action—that the best defense is a good offense—is deeply flawed. In fact, most military and strategic theory holds that the defense is the superior posture.49 For example, Sun Tzu describes controlling an adversary to make their actions more predictable, and hence easy to undermine, by baiting them to attack strong points.50 The stronger form of war is a deception-driven defense: confusing an attacker so that they waste resources attacking strong points that appear weak. This parallels cybersecurity scholars Erik Gartzke and Jon Lindsay's claim that cyberspace is not offense dominant, but deception dominant.51 Rather than persistent action and preemptive strikes on adversary networks, the United States needs persistent deception and defensive counterstrikes optimized to undermine adversary planning and capabilities. Fear and the Security Dilemma New policy options proposed by Cyber Command and the Trump administration risk exacerbating fear in other countries and **creat**ing **a self-reinforcing spiral of tit-for-tat escalations that risk war** even though each actor feels he is acting defensively—or, as it is called in the scholarly literature, a **security dilemma**.52 As shown above, most cyber operations to date have not resulted in escalation. The cyber domain has been a world of spies collecting valuable information and engaging in limited disruptions that substitute for, as well as complement, more conventional options. **Shifting to a policy of preemptive offensive cyber warfare risks provoking fear and overreaction in other states** and possibly producing conflict spirals. Even limited-objective cyber offensive action defined as "defending forward" can be misinterpreted and lead to inadvertent escalation.53 As the historian Cathal Nolan puts it, "intrusions into a state's strategically important networks pose serious risks and are therefore inherently threatening."54 More worryingly, with a more offensive posture, it will be increasingly difficult for states to differentiate between cyber espionage and more damaging degradation operations.55 What the United States calls defending forward, China and Russia will call preemptive strikes. Worse still, this posture will likely lead great powers to assume all network intrusions, including espionage, are preparing the environment for follow-on offensive strikes. According to cybersecurity scholar Ben Buchanan, "in the [aggressor] state's own view, such moves are clearly defensive, merely ensuring that its military will have the strength and flexibility to meet whatever comes its way. Yet potential adversaries are unlikely to share this perspective."56 The new strategy risks **producing a "forever cyber war" prone to inadvertent escalation because it implies all cyber operations should be interpreted as escalatory by adversaries.57** The Myth of Decisive Cyber Victory There is a tendency in the military profession, at least in the United States and Europe, to uphold the concept of decisive battle as central to the Western way of war.58 Often, disruptive technologies—from strategic bombers in the mid-20th century to cyber operations in the 21st century—are seen as providing decisive offensive advantages in crises. In the interwar period between the world wars, airpower enthusiasts argued that bombers would reliably reach their targets, forcing political leaders to end hostilities or face the prospect of destroyed cities and economic collapse.59 Yet the search for decisive battle is often an elusive, if not dangerous, temptation for military planners and policymakers. In a comparative historical treatment of major 19th- and 20th-century battles, Nolan argues that "often, war results in something clouded, neither triumph nor defeat. It is an arena of grey outcomes, partial and ambiguous resolution of disputes and causes that led to the choice of force as an instrument of policy in the first place."60 Decisive victories in any one battle are rare. Adversaries can refuse to fight.61 They can even signal resolve through demonstrating their ability to endure pain. Planning and Assessment Pathologies The new policy framework for offensive cyber operations risks compounding common pathologies associated with strategic assessments and planning. 62 Removing interagency checks increases the risks that an operation will backfire on the attacker or compromise ongoing operations. Misperception is pervasive in insulated decisionmaking processes for several reasons.63 **First, small groups unchecked by bureaucracy tend to produce narrow plans prone to escalation during crises.**64 Second, **leaders often give guidance to planners during crises that reflects their political bias or personality traits rather than a rational assessment of threats and options.65 Third, offensive bias in planning may have little to do with the actual threat and more to do with a cult of the offensive and the desire of officers to ensure their autonomy and resources.66 Removing interagency checks therefore risks compounding fundamental attribution errors and other implicit biases.** Cyber operations are too important to be left to the generals at Cyber Command alone. An Alternative Approach: Cyber Defense-in-Being Rather than going on the offensive, the United States should develop a cyber posture that signals **restraint** and builds an active **defense** network. This network should adopt key tenets of Julian Corbett's concept of a "fleet-in-being." For Corbett, writing in 1911, the operative strategic problem for the British Empire was securing global interests. Regional adversaries could overwhelm local defenses and achieve fait accompli victories, and the British could not be everywhere at once. They had to adopt a fleet-in-being, a distributed network of cruisers (mobility) and fortified ports (strong points) that increased the costs of adversary aggression, buying time for diplomacy and, should it fail, for mobilizing sufficient forces for a counterattack. This dispersed network signaled resolve and generated options by disputing who could command the seas. A fleet-in-being "endeavor[ed] by active defensive operations to prevent the enemy either securing or exercising control for the objects he has in view." This strategy thus advocated "avoiding decisive action by strategical or tactical activity, so as to keep our fleet-in-being till the situation develops in our favor."67 In cyber operations, the United States requires a global network organized around active defenses rather than offensive actions designed to preempt other great powers. This network requires intelligence sharing and target hardening with partners, including industry, to reduce adversaries' expected benefits of cyber operations. Just as new technologies enabled new theories of victory for Corbett, digital connectivity puts a premium on deception and active defense in cyberspace. Active Defense In military theory, active defense is "the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."68 The term comes from Chinese strategic theory and calls for a defensive posture that "strik[es] only after the opponent has struck first."69 In the cyber context, active defense utilizes deception to expose the attacker's espionage and offensive operations in order prepare counterattacks.70 With respect to persistent engagement, defending forward risks undermining the ability to isolate adversary capabilities and, if need be, degrade them through targeted counterattacks designed to limit escalation risks. Deception and defense produce a position of advantage.71 A connected society is inherently vulnerable. New hardware and endless software updates produce new vulnerabilities at a continual, even if variable, rate. The only true security comes from making adversaries doubt the wisdom of attack. One technique that can be used to this effect is to lure would-be attackers into network traps, undermining their confidence in their own intelligence and capabilities. For example, a honeypot is false data that adversaries find so alluring that they attempt to access it. This allows defenders to either identify adversary cyber espionage capabilities or deliver their own payloads to rival networks. Thus, through deception, active defense can change the expected benefits of offensive cyber operations and effectively deter adversaries. The opposition must worry that all of their cyber espionage operations might be revealed, or worse, used as vectors for a counterattack. Hardening Targets **Target hardening** is a concept that emerged in the early Cold War. Based on a 1954 study on the vulnerability of U.S. forces,72 Albert Wohlstetter and Fred Hoffman advocated, among other things, that U.S. forces use passive measures (geographic dispersion, constantly airborne platforms, etc.) and active measures (hardened silos) to reduce vulnerability and ensure a "delicate balance of terror."73 In cyberspace, target hardening also involves active and passive measures.74 In addition to active defense, active measures include investments in human capital and new technology that make it more difficult to access a network. These can range from employing "white hat" hackers, ethical computer hackers who penetrate systems in order to identify vulnerabilities, to updating cyber defensive systems regularly. Passive measures can range from education (e.g., the importance of updating software and avoiding suspicious messages and websites) to ensuring accounts have two-factor authentication—measures that minimize the number of easy attack vectors. If the goal of the recently released National Cyber Strategy is cost-imposition—increasing the costs of enemy activity—the question is how best to alter a rival's cost-benefit calculation in cyberspace. The current strategy relies on offense: operating forward to thwart attacks preemptively. In theory, a rival is deterred by the expectation of punishment for accessing U.S. networks. Yet, an alternative approach would be to adopt a defensive form of cost imposition by targeting hardening and increasing the marginal cost of gaining access to the system. That is, if rivals want to gain access to a network they have to invest more resources and take advantage of more complex—and rare—vulnerabilities. Cost imposition in defense starts with target hardening, and worryingly, the United States has **neglected** this important measure. As a recent Government Accountability Office report makes clear, the Department of Defense has not prioritized **security** in **weapons systems** and there are weaknesses throughout the **entire infrastructure**.75 According to the study, "from 2012–2017, DOD testers routinely found mission-critical cyber vulnerabilities in nearly all weapon systems that were under development. Using relatively simple tools and techniques, tests were able to take control of these systems and largely operate undetected."76 The Pentagon should address these deficiencies and increase the expected costs of gaining access to U.S.—and allied—networks. In cyber operations, the more money adversaries must spend on accessing and exploiting a key network, such as the critical infrastructure of the financial system, the less money they have to spend on conducting other attacks. Coupled with active defense and the use of deception to undermine adversary confidence in their offensive and espionage efforts, target hardening changes the projected benefits of cyber operations. Defensive options, such as hardening targets and increasing societal resiliency, ensure the target is difficult to coerce. As Buchanan notes, "no cybersecurity approach is credible unless it begins with a discussion of the vital role of baseline defenses."77 These defenses, consistent with the Department of Homeland Security strategy, start with "identifying the most critical systems and prioritizing protection around those systems."78 Cyber strategy should prioritize hardening key targets while seeding the network with digital traps—active defenses—that undermine adversary offensive and espionage options. Intelligence Sharing and Coordination There are also benefits to sharing threat intelligence with industry and allies. The United States operates a global security network that connects not just treaty allies but businesses and civil society actors.79 Any cyber strategy must embrace this fact as a source of strength, not a point of vulnerability. A greater number of actors identifying adversary cyber operations provides early warning indicators and reveals adversary capabilities. To date, intelligence sharing associated with cyber operations has been prone to interagency debate and coordination challenges. There are organizational seams, such as the divide between the FBI and CIA before the September 11th terrorist attacks, that often limit intelligence sharing and create barriers to effective response within the federal government.80 This dilemma is compounded with respect to alliance partners and industry. States and many other organizations tend to stovepipe information and undermine effective coordination based on security risks. Yet, closing off information in a

network limits responsiveness. Rather than limit information sharing, the United States should reengage processes such as the Obama administration's Vulnerabilities Equities Policy, which sought disclosures of newly discovered and unknown malware that might pose a global threat.81 Sharing threat intelligence is central to not just interagency coordination, but working with partner states, businesses, and civil society. In order to strengthen the defense of the network through depth, the United States will need to assume risk in sharing information, and hence lose some offensive options. This includes working with nontraditional actors, such as the white hat hacker community, which conducts probes in order to help strengthen networks from adversary attacks.82 It also implies sacrificing some espionage and offensive cyber options to ensure partners can patch their networks and update their defenses. Conclusion Cyber policy and strategy should favor restraint over offense in protecting the digital commons. In MIT political scientist Barry Posen's proposed grand strategy, restraint calls for fewer forward-deployed forces and less coordination with partners.83 In a cybersecurity context, restraint implies preserving the digital commons for commercial and social interests, thus limiting military action to the greatest extent possible. **Restraint can also help shape norms in cyberspace and make escalation taboo.8**4 To date, restraint has largely been the prevailing norm in this domain. Restraint has prevailed not so much as a prescribed foreign policy strategy, but because more aggressive tactics are ineffective, and states therefore use them sparingly.85 Data on cyber actions from 2000 to 2016 suggest a restrained domain with few aggressive attacks that seek a dramatic impact. Attacks do not beget attacks, nor do they deter them. The policy discourse is inconsistent with these observations. If few operations are effective in manipulating the enemy and fewer still lead to responses in the domain, why would a policy of offensive operations be useful in cyberspace? For a variety of reasons, including the ineffectiveness of cyber operations and the fear of weapons proliferation, a normative system of restraint has gradually emerged in cyberspace. A policy of restraint that maintains control over the weapons of cyber war is therefore appropriate and strategically wise. **Loosening the rules** of engagement in **pursuit of a more offensive posture**, as the **Trump** administration advocates, **violates norms** and can lead to disastrous consequences for the entire system. Given the ambiguous nature of signals in cyberspace, it is difficult to be sure that an offensive operation will be correctly interpreted as a warning shot designed to get adversaries to back down. Platitudes like "the best defense is a good offense" are best left for sports, not international politics. The evidence suggests that in cyberspace, **the best defense is actually a good defense.**

Popik '17 quantifies that:

Thomas S. Popik, 6-22-2017, "TESTIMONY OF THE FOUNDATION FOR RESILIENT SOCIETIES," FEDERAL ENERGY REGULATORY COMMISSION, https://www.climateviews.com/uploads/6/0/1/0/60100361/popik_thomas_testimony_ferc_technical_conference_june_22_2017_resubmitted.pdf

What is a long-term and large-scale disruption to the bulk power system? It is a blackout that: 1. Persists longer than the supplies of backup energy necessary for grid restoration. 2. Covers a geographic area so large that significant outside assistance is impractical. **If a region of the United States were to experience a** long-term and **large-scale disruption of the bulk power system,** other dependent critical infrastructures would likewise be disrupted. Human casualties could be very high, both in percentage terms and in absolute numbers. Recovery could take months or years. Over a large area, **deaths could be in the millions**.

And A successful cyber-attack causes a great power war. Miller '17,

[James N. Miller and Richard Fontaine, 9-19-2017, A New Era in U.S.-Russian Strategic Stability, Center for a New American Security, https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNASReport-ProjectPathways-Finalb.pdf] // MA

As was the case in the Cold War, the most plausible scenario for U.S. and Russian military forces to engage in large-scale combat is in Europe. It is worth considering first how even a very limited attack or incident could set both sides on a slippery slope to rapid escalation. If armed conflict looks at all likely, both sides would have overwhelming incentives to go early with offensive cyber and counter-space capabilities to negate the other side's military capabilities or advantages. If these early cyber and space attacks succeed, it could result in huge military and coercive advantage for the attacker – with few or even no direct casualties. It may appear very unlikely that the attacked side would retaliate strongly in response to some damaged computers and some malfunctioning satellites in outer space. Moreover, if the attacks fail to have the desired effect, the other side may not even notice. Large-scale **cyber** and space **attacks** – preferably before a kinetic conflict even starts – therefore may **appear** a **low-risk**, high-payoff move for both sides. LIMITED CYBER AND SPACE ATTACKS WITH CASCADING EFFECTS ON CIVIL SOCIETY **With each side having emplaced cyberimplants to disrupt or destroy the other side's military systems and critical infrastructure –** including war-supporting infrastructure as well as purely civilian infrastructure, **a small spark in cyberspace could rapidly escalate**. The spark could come **from** an intentional cyber attack that had **unintended cascading effects, or from proxies or false flag attacks**. Thus, cyber and space attacks intended to be highly discriminative

against military targets may cascade to affect critical infrastructure essential to the broader society and economy. If this occurred, **an attack intended to be precise** and limited to military targets instead **could result in the widespread loss of electrical power, water**, or other **essential services, with resulting economic disruption and potential loss of life.** The attacked side could feel compelled to respond at least in kind. Alternatively, **a tit-for-tat cycle may occur**, as **one side** may **believe it could gain coercive advantage** by intentionally demonstrating its ability to hold at risk the other side's critical infrastructure through cyber, counter-space, and perhaps sabotage attacks. There is debate within the expert community as to whether cyber attacks alone could have devastating effects, but it does appear likely that combined cyber and precision attacks on critical infrastructure could devastate an economy and society. Whether such **attacks escalated through a gradual tit-for-tat or more rapid counterpunching, such counter-value strikes could lead to major conflict and** potentially **nuclear war**.

Cross x clare 23 from c1 for great power war casuing extinction

Contention 3 is Sudan

The Sudanese military is using chemical warfare now. Walsh 25 finds

Walsh 1/16 [Declan Walsh, chief Africa correspondent for The Times, 1-16-2025, Sudan's Military Has Used Chemical Weapons Twice, U.S. Officials Say, NYT, https://www.nytimes.com/2025/01/16/world/africa/sudan-chemical-weapons-sanctions.html, //RR]

Sudan's military has used chemical weapons on at least two occasions against the paramilitary group it is battling for control of the country, four senior United States officials said on Thursday. The weapons were deployed recently in remote areas of Sudan, and targeted members of the Rapid Support Forces paramilitaries that the army has been fighting since April 2023. But U.S. officials worry the weapons could soon be used in densely populated parts of the capital, Khartoum. The revelations about chemical weapons came as the United States announced sanctions on Thursday against the Sudanese military chief, Gen. Abdel Fattah al-Burhan, for **documented atrocities by his troops, including indiscriminate bombing of civilians and the use of starvation as a weapon** of war. The use of chemical weapons crosses yet another boundary in the war between the Sudanese military and the R.S.F., its former ally. By many measures, **the conflict in Sudan has** created the world's **worst humanitarian crisis**, with as many as **150,000 people killed**, over **11 million** displaced and now the world's **worst famine in decades**. "Under Burhan's leadership, the S.A.F.'s war tactics have included **indiscriminate bombing** of civilian infrastructure, attacks on **schools, markets**, and **hospitals**, and **extrajudicial executions**," the Treasury Department said, using an acronym for Sudan's armed forces. General al-Burhan responded with defiance: "We are ready to face any sanctions for the sake of serving this nation, and we welcome them," he told reporters during a visit to El Gezira state. The U.S. decision is considered a significant move against a figure seen by some as Sudan's de facto wartime leader, who also represents his country at the United Nations. Aid **groups fear that Sudan's military could retaliate against the sanctions** by further restricting aid operations in areas that are either in famine or sliding toward it. The decision could also reshape broader relations between Sudan and the United States, whose Sudan envoy, Tom Perriello, has been a leading figure in the faltering efforts to reach a peace deal. Although chemical weapons were not mentioned in the official sanctions notice on Thursday, several U.S. officials said they were a key factor in the decision to move against General al-Burhan. Two officials briefed on the matter said the chemical weapons appeared to use chlorine gas. When used as a weapon, chlorine can cause lasting damage to human tissue. In confined spaces it can displace breathable air, leading to suffocation and death. Knowledge of the chemical weapons program in Sudan was **limited to a small group** inside the country's military, two of the U.S. officials said, speaking on the condition of anonymity to discuss sensitive security matters. But it was clear that General al-Burhan had authorized their use, they said. Sudan's ambassador to the United Nations, Al-Harith Idriss al-Harith Mohamed, said in a text message that Sudan's military had "never used chemical or incendiary weapons." "On the contrary, it's the militia that used them," he added, referring to the Rapid Support Forces. Last

week, the United States determined that the Rapid Support Forces had committed genocide in the war and imposed sanctions on its leader, Lt. Gen. Mohamed Hamdan, for his role in atrocities against his own people. The United States also sanctioned seven companies based in the United Arab Emirates that traded in weapons or gold for the R.S.F. Sudan's military has been accused of using chemical weapons before. In 2016, Amnesty International said it had credible evidence of at least 30 likely attacks that killed and maimed hundreds of people, including children, in the western Darfur region. The organization published photos of children covered in lesions and blisters, some vomiting blood or unable to breathe. As the United States debated punitive measures against General al-Burhan last week, the Sudanese authorities announced that they would maintain a major aid corridor through neighboring Chad, a move American officials saw as an effort to avoid the sanctions. But the evidence of chemical weapons was **too compelling to ignore,** several U.S. officials said. The United States detected numerous chemical weapons tests by Sudanese forces this year, as well as two instances in the past four months in which the weapons were used against R.S.F. troops, two of the officials said. The United States also obtained intelligence that chemical weapons could soon be used in Bahri, in northern Khartoum, where fierce battles have raged in recent months as the two sides compete for control of the capital. **Chlorine** was first weaponized during World War I, and its use in combat **is prohibited by international law.** In the mid-2000s, insurgents in Iraq weaponized chlorine in attacks on U.S. troops. It has also been used in improvised bombs by ISIS fighters and by the Assad regime in Syria.

That's because the ICC lacks sufficient funding. Coalition for ICC 22 finds

Coalition for ICC 22 [Victims could lose out with states' double-standard on International Criminal Court resources", No Publication, https://coalitionfortheicc.org/news/20220330/OpenLetter_ICCresources] //RR

The Coalition for the International Criminal Court (Coalition) welcomes the renewal of support for the critical role of the International Criminal Court (ICC) to deliver justice for serious international crimes, and the expressions of interest by its States Parties in bolstering the financial and human resources of the Court. While the positive response of States Parties signals a commitment to justice, States Parties' **chronic underfunding of the Court has led** to an exceptional request by the Office of the Prosecutor for voluntary contributions to be provided outside the Court's regular budget, including through a newly established trust fund and gratis personnel. The Coalition has repeatedly called attention **to the significant** and long-standing **gap between the Court's workload and** the **resources available to it in its regular budget. The Court's budget has consistently been limited by States Parties, including through the insistence of some on "zero nominal growth"** and in setting arbitrary financial envelopes, including for legal aid, and by failures on several occasions of the Court to request the resources it needs. **This has impacted the Court's effectiveness and delayed victims' access to justice.** This recent call by the Office of the Prosecutor to States Parties for voluntary contributions and gratis personnel to support its investigative activities – and the enthusiastic response by some States Parties – amounts to an admission by the Court and its States Parties that the Court does not have adequate resources**. The call for voluntary contributions** and gratis personnel when attention is high on one specific situation also **risks exacerbating perceptions of politicization of and selectivity in the Court's work.** Recent pledges by States Parties of **funding** and seconded personnel in the context of a specific situation sends the unfortunate signal that justice for some victims should be prioritized over others, depending on political will, including a willingness to make resources available. States Parties should be alert to the fact that perceptions of **selectivity** in the prioritization of **situations** or inappropriate bias in the Court's work **are detrimental to the Court's legitimacy and** can undermine the **credibility** of the justice it renders where it does act. The Court's States Parties collectively share responsibility for ensuring appropriate resources for the entire Court through setting its annual budget. This provides the best protection for prosecutorial and judicial independence by ensuring sufficient budgetary resources are available for the Court to take and implement decisions by reference only to the applicable law and to the fairness of proceedings. Voluntary contributions to the Office of the Prosecutor will not address the resource needs of other organs, parties and participants, which increase in correlation with the Office's activities. **Voluntary contributions** also **raise significant risks when it comes to the sustainability of funding.** In addition, there are policy considerations in the use of gratis personnel, including perceptions that seconded personnel may have divided loyalties.

Affirming solves - the US would by law would have to provide a substantial increase to the mandatory fund. Brahm 23

Brahm 23 [Eric Wiebelhaus-Brahm, 1-31-2023, "The evolution of funding for the International Criminal Court: Budgets, donors and gender justice", Taylor & Francis, https://www.tandfonline.com/doi/full/10.1080/14754835.2022.2156276 // RR]

Once the overall budget is set, state parties' individual contributions are calculated. During treaty negotiations, there was a proposal to fund the Court through the United Nations. The primary opponents were the United Nations's biggest contributors—namely the United States, Germany, and Japan—and the idea was abandoned (Schabas, Citation2020). However, assessed contributions for the Court are calculated in the same way as for the United Nations. **Per Article 117 of the Rome Statute, "contributions of States Parties shall be assessed in accordance with an agreed scale of assessment, based on the scale adopted by the United Nations for its regular budget and adjusted in accordance with the principles on which that scale is based." In other words, states are assigned a proportion of the overall budget that is essentially based on the size of their economies. As such, our data available on the Harvard Dataverse site show that the ICC's largest funders are large European economies, Japan, South Korea, Australia, and Brazil.**

AND Trump pressures international organizations' partners to spend. This has been empirically seen in NATO. CNBC 25'

CNBC on 1/23 reports Holly Ellyatt, 1-23-2025, "Can Trump force the hand of NATO allies to spend up to 5% of GDP on defense?", CNBC, https://www.cnbc.com/2025/01/23/can-trump-get-nato-allies-to-spend-more-on-defense.html //RR

As U.S. President Donald **Trump looks to immediately fix** his greatest political and economic bugbears, the thorny issue of **NATO defense spending** is likely to quickly return to the global fore. Trump's relationship with the Western military alliance was acrimonious during his first presidency, with the Republican leader frequently lambasting NATO member states for not abiding by a 2014 target to spend at least 2% of GDP on defense every year. Ahead of his second term in office, Trump signaled that the debate over military spending — and Trump's perception that NATO members are over-reliant on the U.S. for their own security — will be back on the agenda, stating that NATO's 32 member countries should contribute even more toward defense. "I think NATO should have 5% [of their GDP as a NATO contribution target]," he said in January. "They can all afford it, but they should be at 5%, not 2%", he said at a press conference in which he also refused to rule out using military force to seize the Panama Canal or Greenland — a territory that belongs to NATO member Denmark. **There has been a** broad **increase in defense expenditure among NATO members since Trump was last in power.** In 2018, at the height of the White House leader's irritation with the military bloc, only six member states met even the 2% of GDP target. By contrast, NATO data estimates that 23 members met the 2% target in 2024. While some surpassed that threshold — such as Poland, Estonia, the U.S., Latvia and Greece — major economic powers including Canada, Spain and Italy are among the laggards below the contribution threshold. No NATO member has reached a 5% target suggested by Trump, including Washington under the administration of his predecessor Joe Biden. Europe must return to 'Cold War-era defense expenditure policies,' says Polish Presidentwatch now VIDEO08:30 Europe must return to 'Cold War-era' defense policies, says Polish President Polish President Andrzej Duda fully supported Trump's call for higher spending across NATO, telling CNBC on Wednesday that it was "paramount" that Europe returns to Cold War-era defense spending to defend against the likes of Russia and its expansionist foreign policy. "If we want to defend against this – and us Poles decisively do – we're spending close to 5% of GDP on defense this year. We're aware that we have to modernize our armed forces, we have to be strong and provide a real deterrent to keep Russia aggression at bay," he told CNBC's Steve Sedgwick on Wednesday on the sidelines of the World Economic Forum in Davos, Switzerland. Perhaps understandably, given that it borders war-torn Ukraine, Poland spends the highest proportion of its GDP on defense compared to other NATO members. The NATO 2024 estimates suggest Warsaw spent 4.12% of its GDP on defense last year. New leader, old problems? The Netherlands' former Prime Minister Mark Rutte, now the secretary-general of NATO, is only a few months into his new job, but he has already repeatedly called on member states to increase defense spending. His priority, however, is to get laggard countries to reach the 2% target, he said. "Luckily, thanks to Trump in his first term, we have stepped up defense spending. ... but we all have to get to the 2%," he told CNBC's Steve Sedgwick at the World Economic Forum in Davos on Thursday. Countries that have still not reached the requisite target "have to get to 2% in the coming months. It has to be done this year," noted Rutte, who has himself faced flak over why Dutch defense spending was below the NATO target for much of his time in office.

That's specifically key for Sudan. As they have become the victim of budget cuts. The ICC budget for 2025 states

International Criminal Court, 07-24-2024, "", Assembly of State Parties 23rd Session, https://asp.icc-cpi.int/sites/default/files/asp_docs/ICC-ASP-23-10-AV-ENG.pdf //RR

The Court's external offices have requested an amount of €353.2 thousand, representing a decrease of €26.8 thousand (7.1 per cent) as compared with the resources approved for 2024. The resources requested by the country offices/field presences are required to purchase consumable items to support day-to-day operations, including fuel for vehicles and generators, office supplies, light IT equipment, air conditioners, drinking water, emergency rations and personal protection equipment (PPE) to be used by field staff. The amount requested by the Country Office (Ukraine) (€75.0 thousand) has

increased by €5.5 thousand (7.9 per cent) as compared with the resources approved for 2024 due to increased operational costs for managing a larger fleet of vehicles, fuel consumption and increased in country missions planned by OTP. The Ukrainian electricity infrastructure, power plants and networks have been subject to repeated attack and it is therefore anticipated that the Country Office (Ukraine) will require more fuel for its electricity generator in 2025. The Country Office (Ukraine) also needs to purchase more emergency rations, water and office supplies in 2025 to cover the greater need for operational, logistical and security support. The increase requested by the Country Office (Central African Republic) results from the reintegration of the costs of support (flights, vehicles, internet) by MINUSCA to the missions scheduled by VPRS, CMS, OPCV, SSS, TFV and PIOS outside Bangui. These costs were included in the budgets of Headquarters sections for 2024. **The increase requested by the** country **offices in Ukraine and the CAR has been completely offset by** the **reductions identified in** Côte d'Ivoire, Uganda, the DRC and **Sudan** resulting from reduced consumption **because of a reduction in activity as well as the scaling down of the Court's presence.**

That's detrimental as the ongoing Sudanese conflict risks regional instability and state collapse. Crisis Group writes that

Crisis Group, 5-6-2023, "Time to Try Again to End Sudan's War," Crisis Group, https://www.crisisgroup.org/africa/horn-africa/sudan/time-try-again-end-sudans-war, accessed: 3-29-2024 //MA

The imperative of ending this ugly war does not obscure the fact that any ceasefire and deal between these two deeply discredited belligerents would be unpalatable to many Sudanese – and could be difficult to enforce on the ground. The two sides, especially the RSF, have committed horrendous atrocities. The army has repeatedly bombed crowded Khartoum neighbourhoods. **The RSF and its allies, meanwhile, have engaged in wanton pillage and, residents say, sexual violence against women and girls as well as other grave abuses in Khartoum and elsewhere.** In Darfur, whence many of the paramilitary forces come**,** the RSF and affiliated militias stand credibly accused of killing thousands of civilians and uprooting tens of thousands more from their homes (after fighting broke out between RSF- and army-aligned communities), in brutality reminiscent of previous atrocities in the stricken western region. Yet **the alternative to a** negotiated **end** to fighting **is** more war, and more **suffering, for Sudanese and a wider state collapse that could engulf the Horn of Africa and the Sahel.** The Cost of More War Sudan's war was decades in the making. In its post-colonial history, the country has veered from military dictatorship to democracy and back again, in a cycle replete with hope-filled popular uprisings and coups. Meanwhile, far from the riverine centre, war has wracked much of the country's periphery almost continuously. In the most recent episode, Sudanese peacefully took to streets throughout the country in late 2018 and 2019 to oust Bashir, who had grabbed power in a 1989 coup. Sudan's generals stepped in to seize control. The result was an awkward power-sharing arrangement, with Burhan as chair of a transitional government and Hemedti as his deputy. Both promised to hand over the reins to civilians but in practice worked to consolidate their own hold, including through an October 2021 coup that derailed the transition, to the enormous frustration of both Sudanese and sympathisers abroad. Yet the marriage of convenience began to fray. Hemedti and his paramilitary force, which grew out of the Arab-identifying militias Bashir armed to fight his dirty wars in the western hinterlands, became ever more ascendant. Eventually, the relationship reached a breaking point as Hemedti threw in his lot with a group of civilians after a December 2022 deal to restore civilian rule. As a dispute escalated over when and under which leadership structure Hemedti would integrate his irregulars into the army chain of command, both leaders made a show of force, flooding Khartoum with fighters. The shooting started on 15 April. Khartoum is destroyed, and most Sudanese with the means to flee have done so. Many have nothing to come home to. The consequences will likely reverberate for decades. Khartoum is destroyed, and most Sudanese with the means to flee have done so. Many have nothing to come home to, with the RSF in particular looting residential neighbourhoods and occupying homes, seizing what they consider the booty of war. The power vacuum at the country's centre is felt elsewhere - most sharply in Darfur, where both the RSF and the army have mobilised tribal militias, exacerbating longstanding conflict between Arab- and non-Arab-identifying communities. Attacks by the RSF and associated militias have led to the death and displacement of thousands of civilians, mostly from the Masalit community, many of whom have fled across the border into Chad, leaving West Darfur under RSF control. South Sudan-aligned rebels in the south of the country are again on the march. **Many suspect it is only a matter of time before trouble also appears in eastern parts of the country.** Unless there is a deal to reconsolidate state power, **these conflicts will** likely **continue to spiral**. If the Sudanese army is defeated or disintegrates**, the country will be** without a national army (dubious as the present force's claim to that title may be) and **in the full control of** an unprofessional, violent **paramilitary force** with a pronounced ethnic cast. Moreover, the army may break apart, with sections of it fighting on. It is unclear in what form the Sudanese state (long controlled by the riverine centre) would survive in such circumstances. Meanwhile**,** the longer the war drags on, the deeper **other parts of Sudan will sink into local strife, heightening the possibility of intervention by outside powers and further destabilising Sudan's neighbourhood**. Time for a Coordinated Push In order for peace talks to succeed, both parties will have to see an upside to reaching a deal, and outside actors will need to provide a coherent, well-supported negotiating track. Right now, it is unclear what the former might entail or even whether anything can compel the army and RSF to negotiate rather than fight. The latter has yet to come together.

It causes a regional draw-in Darwich 23

May Darwich (Associate Professor of International Relations of the Middle East, University of Birmingham), 5-4-2023, "Sudan: the longer the conflict lasts, the higher the risk of a regional war," Conversation, https://theconversation.com/sudan-the-longer-the-conflict-lasts-the-higher-the-risk-of-a-regional-war-204931, accessed: 3-27-2024 //ZD

The Sudanese armed forces and a paramilitary force known as the Rapid Support Forces have declared war against each other, bringing the country to its knees. The main protagonists are two generals: Abdel Fattah al-Burhan, who leads the armed forces, and Mohamad Hamdan Dagalo (known as Hemedti) of the Rapid Support Forces. The hostilities have been most intense in the capital city, Khartoum. But violence has broken out in other provinces and is threatening to revive long-simmering violence in Darfur. **There is** also a **risk that the conflict could spill over** to neighbouring countrie**s and escalate into a regional conflict.** Geographically, Sudan borders seven countries: Chad, the Central African Republic (CAR), South Sudan, Egypt, Eritrea, Ethiopia and Libya. Politically and culturally, **it straddles the Middle East, north Africa and the Horn of Africa**. Regional powers and neighbours have lined up behind either of the two generals – or in some cases both. **Egypt and Saudi Arabia have been backing al-Burhan. For their part, the United Arab Emirates (UAE) and General Khalifa Haftar of Libya have supported the Rapid Support Forces**. But many other actors remain undecided. There is a real possibility that regional and **international actors will be arming different sides** as they pursue their own, often competing interests. **This could bring unprecedented shifts in the region's** already **uneasy** regional **equilibrium**, and test pre-existing alliances. Regional and international actors are key in enabling – or preventing – the development of the crisis into a protracted civil war with regional dimensions. The best chance of halting Sudan's slide into civil war lies in a united front of Western and regional powers, with Sudanese civil society groups putting pressure on the warring generals for a permanent ceasefire. And a return to a civilian-led transition. But as time goes by, many despair that Sudan will soon reach the point of no return. Fretful neighbours Egypt: **Egypt had a long history of meddling in Sudan's affairs**. This has included supporting various military governments, as well as containing the Islamist resurgence in the 1990s. In 2019, when al-Bashir was deposed, Egypt supported al-Burhan in the transition. It didn't want a military regime – and its ally – being replaced by a civilian democratic government. It feared that this would inspire Egyptians to do the same. Since the outbreak of the recent conflict, Egypt has adopted a cautious approach by working to mediate a permanent ceasefire. This is because the war brings risks. It is already having to manage a refugee crisis as tens of thousands of Sudanese attempt to get away from the conflict. In addition, an **escalation of the conflict could potentially bring instability to Egypt's southern borders**. This could open up routes for arms smuggling and illegal trade. Also, **Egypt may be goaded to get involved militarily if the fighting continues.** But, Egypt's greatest fear must be that it will lose its main ally in the ongoing disagreement with Ethiopia over the operation of the Grand Ethiopian Renaissance Dam (GERD), situated on the Blue Nile river near Ethiopia's border with Sudan. The conflict will complicate the management of the dam, as both generals may have different views on the issue. **A prolonged conflict in Sudan could have long consequences for Egypt's food and water security**. Ethiopia: Relations with Sudan have been strained in recent years due to border disputes over land claims and disagreements over the GERD. **A protracted conflict in Sudan could have an effect on border disputes**. These disputes are connected to tensions over the contested fertile farmland of Al Fashaga and apparent Sudanese support for Tigrayan opponents against the Ethiopian federal government. The crisis in Sudan may affect the equilibrium on these border issues. **On Sudan's western frontiers, Libya, Chad and CAR risk spill overs from violence and tensions in the Darfur region**. Hemedti is a tribal leader from the Mahariya clan of Darfur's Rizeigat tribe. He has been a main partner to Haftar of Libya in trading drugs, arms and refugees across borders between Sudan, Libya and Chad. With tensions rising in Darfur, forces could be split: some will side with Hemedti's forces. Others will seek to undermine them. External powers In civil wars in the Middle East and Africa, such as in Syria, Iraq, Libya and Yemen, international actors have intervened by replenishing their allies with weapons, sponsoring diplomacy involving the warring groups, and sometimes taking matters into their own hands by launching military interventions. Clashes in **Sudan could very well turn the region into a playground for external powers** to extend their influence. Under presidents Barack Obama and Donald Trump, US influence waned across Africa and the Middle East. At the same time, America's competitors took steps to carve out a strategic foothold in the Horn of Africa and the critical maritime route of the Red Sea. **Russia**, for example, is reportedly negotiating military and economic deals, allowing it to use Sudan's ports on the main trading routes to Europe. There have also been accusations that Russia's Wagner Group is involved in illicit gold mining in Sudan. For its part **China**, Sudan's second-largest trading partner (after Saudi Arabia), has invested heavily in infrastructure and oil extraction, giving it an important stake in the conflict. Wealthy oil producers – Saudi Arabia and the UAE – have an interest in establishing regional dominance. The UAE, aspiring to control maritime routes in the Gulf of Aden and the Red Sea, has taken serious interest in ports in Sudan. For its part, **Saudi Arabia has been keen to prevent Iran from establishing a foothold in Sudan. As a result, it has poured money into supporting Sudan's military.** Both interfered to shape the 2019 transition in Sudan to ensure a friendly regime would end up in power. And both invested in a range of economic and

military enterprises. But they haven't been supporting the same general: **Saudi Arabia has supported al-Burhan while the UAE** has been an ardent **support**er of **Hemedti**. **The longer the conflict continues, the greater the odds for a longer, bloody war with regional and international entanglements.** This will **make it more difficult to contain the conflict** or find a resolution that satisfies all parties.

Cross x clare 23 from c1 for great power war causing extinction

2AC

1. Ceasefire alr failing

Adam **Kredo**, 20**25**-02-10, "Hamas Says It Will Stop Releasing Israeli Hostages, Putting Tenuous Ceasefire Deal on Cusp of Collapse," No Publication, https://freebeacon.com/israel/hamas-says-it-will-stop-releasing-israeli-hostages-putting-tenuous-ceasefire-deal-on-cusp-of-collapse/, Date Accessed: 2025-02-17T04:31:24.542Z //RX

Hamas announced on Monday that it **would not move forward with the next scheduled release of Israeli hostages**, citing the Jewish state's purported "violations" of a tenuous ceasefire deal that is on the cusp of unraveling. The announcement comes after **Hamas paraded several gaunt Israeli hostages** across a stage in Gaza this weekend, drawing shocked reactions from the Israeli public and President Donald Trump. A spokesman for Hamas's military wing, Abu Obeida, **accused Israel of failing to stick to the terms** set forth under a three-tiered ceasefire agreement, which is approaching the end of its first phase. Hamas claims that Israel is not allowing displaced Gazans to return home and that it is still conducting military operations in the territory. The terrorist outfit did not provide evidence. The move threatens to upend a ceasefire deal that was already fraying due to Hamas's brutal treatment of the hostages it has already released. It also comes a week after Trump unveiled ambitious plans to take control of the Gaza Strip and turn it into the "Riviera of the Middle East." The hostages remain Hamas's only bargaining chip, and without their return, Israel could restart full-fledged military operations in Gaza. Defense Minister Israel Katz did not say he would do so when he responded to Hamas's announcement on Monday, though he did say he directed Israel's military "to prepare on highest alert for every possible scenario in Gaza."

2. 1NC Shamin is just powertagged -- it actually says that it could cause Western states to <u>choose</u> to stop weapons, not that the ICC actually <u>forces</u> stopping weapons

Shamim 24 [Sarah Shamim is a reporting fellow at the Pulitzer Center. "Arms to Israel: Will Countries Halt Sales in Wake of ICC Arrest Warrants?" *Al Jazeera*, Al Jazeera, 22 Nov. 2024, www.aljazeera.com/news/2024/11/22/arms-to-israel-will-countries-halt-sales-in-wake-of-icc-arrest-warrants. DOA: December 29, 2024 // harris //recut TH] recut //RX

Western nations which sell arms to Israel may be forced to re-evaluate their trade agreements after arrest warrants issued by the International Criminal Court (ICC) against Israeli Prime Minister Benjamin Netanyahu and his former Defense Minister Yoav Gallant for "war crimes" and "crimes against humanity" in Gaza, experts say. The warrants come amid Israel's continuing bombardment and military campaign on the Gaza Strip, where more than 44,000 Palestinians have been killed since October 7, 2023, according to health officials. All 124 countries which are signatories to the Rome Statute of the ICC are now legally obliged to arrest Netanyahu and Gallant if they set foot on their territory. The question of whether countries supplying arms to a country whose leaders are accused of crimes against humanity could be considered complicit is unclear, but experts say some suppliers will have to consider carefully if they wish to continue to support Israel in its war on Gaza. Which countries provide arms to Israel? Stockholm International Peace Research Institute (SIPRI) estimated that between 2019 and 2023, Israel was the 15th largest importer of arms globally. It said the United States, Germany, the United Kingdom, France and Spain export arms to Israel. A United Nations report published on February 23, 2024 says Canada and Australia have also exported weapons to Israel. The US Israel imported 69 percent of its weapons from the US between 2019 and 2023, according to SIPRI. The principle of ensuring that Israel has a "qualitative military edge" was enshrined in US law in 2008. After October 7, 2023, when Israel launched its ongoing assault on the Gaza Strip following a Hamas-led attack on villages and army outposts in southern Israel, the US further ramped up the transfer of weapons to Israel. Last month, Washington announced it would send its advanced Terminal High Altitude Area Defense (THAAD) missile defence system to Israel, along with US soldiers who would operate the system. On Wednesday, the US Senate voted down an effort led by independent Vermont Senator Bernie Sanders to block a series of planned weapons sales to Israel. Sanders introduced the bill against a $20bn weapons deal which had been approved by the administration of President Joe Biden. So far, the US, which is not a signatory to the Rome Statute of the ICC, has shown no signs of being prepared to reduce or halt weapons to Israel. "We fundamentally reject the court's decision to issue arrest warrants for senior Israeli officials," White House spokeswoman Karine Jean-Pierre told reporters. This sentiment was shared by many politicians from both parties in the US. Germany SIPRI estimates weapons sent by Germany constitute 30 percent of Israel's weapon imports, a tenfold rise in 2023 compared with 2022. Germany mostly sends naval equipment to Israel, including frigates and torpedoes. In March, Nicaragua filed a case at the International Court of Justice (ICJ), asking the court to order Germany to immediately stop exporting arms to Israel because "this aid is used or could be used to commit or to facilitate serious violations of the Genocide Convention, international humanitarian law or other peremptory norms of general international law". On April 30, the court rejected the request, saying the monetary value of the weapons for which Germany granted export licences had decreased. In June, several Palestinians in Gaza filed requests to an administrative court in Berlin to stop the German government from exporting weapons. These requests were also rejected. In September, a spokesperson for the German Ministry for Economic Affairs said: "There is no German arms export boycott against Israel." The UK SIPRI data shows that while the UK has not provided Israel with major arms since the 1970s, it has provided components for various systems such as the F-35 combat aircraft. "No lethal or other military equipment has been provided to Israel by the UK Government since 6 December 2023," then-Minister of State for the Armed Forces Leo Docherty told Parliament in April 2024. Official data on export permits in June 2024 showed that 108 licences, for which Israel was listed as a recipient, had been approved since October 7, 2023. In September this year, the UK suspended 30 licences out of a total of 350. These 30 pertained to weapons that the UK believed were being used in military operations in Gaza. Which other countries have restricted arms sales over the course of the war? France According to data by SIPRI, France did not send weapons to Israel between 2018 and 2023, and the last time it sent weapons was in 1988. However, France does supply components used to build weapons. In June, French investigative media website, Disclose, revealed that France had sent electronic equipment for drones suspected of being used to bomb civilians in Gaza. In October, French President Emmanuel Macron told French media: "I think that today, the priority is that we return to a political solution, that we stop delivering weapons to fight in Gaza." He added: "France is not delivering any." Italy SIPRI estimates that Italy's weapons sent to Israel accounted for 0.9 percent of Israel's weapons imports between 2019 and 2023. Italy mostly sent light helicopters and naval guns. The Italian government made repeated assurances that Italy had not sent weapons to Israel since the war broke out. Prime Minister Giorgia Meloni said in the Italian Senate in October this year: "The government immediately suspended all new export licences, and all agreements signed after October 7th [2023] were not implemented." However, in March this year, Italian Defence Minister Guido Crosetto said despite these assurances, Italy had sent some weapons to Israel. Crosetto said these were the weapons for which orders were signed before October 7. Independent Italian media outlet Altreconomia analysed data from statistics agency ISTAT and reported that Italy had sent 2.1 million euros ($2.2m) in arms and munitions to Israel in the last three months of 2023. Spain The Spanish Ministry of Foreign Affairs, European Union and Cooperation issued a news release in February 2024 saying arms sales to Israel had not been authorised since October 7, 2023. Euronews reported that Spanish investigative journalists found that in November 2023, munitions worth 987,000 euros ($1.03m), were sent to Israel under a licence approved before October 7, 2023, however. Canada In February this year, Canadian Foreign Affairs Minister Melanie Joly said Canada would stop all arms shipments to Israel. However, campaigners claimed that Canada was sending weapons to Israel via the US instead. In September, Joly said Canada had suspended 30 permits for arms sales to Israel. It is unclear how many permits in total exist. Joly added that Canada had cancelled a contract with a US company that would sell Quebec-manufactured arms to Israel. Belgium, Japanese company Belgium and a Japanese company have also suspended weapons exports to Israel. How might the ICC arrest warrants affect arms sales to Israel? By issuing the arrest warrants for Netanyahu and Gallant, relating to war crimes and crimes against humanity, "the ICC has also made a certain demand on Western countries both in North America and throughout Europe," Neve Gordon, professor of international law at Queen Mary University of London told Al Jazeera. "And that has to do with the kind of trade agreements that they have with Israel – first and foremost with the trade relating to arms." **He added: "If leaders of Israel are charged with crimes against humanity, then this means that the weapons provided by Western nations are being used to commit crimes against humanity." The ICC decision could** well therefore **lead more** Western **countries to place embargoes on weapons exports to Israel**, Eran Shamir-Borer, the director of the Center for National Security and

Democracy at the Israel Democracy Institute told Israeli newspaper Haaretz. Shamir-Borer was formerly part of the Israeli military. Most countries have a memorandum of arms trade which sets out the conditions under which arms can be traded, Gordon said. In each memorandum, a provision clearly states that the country "cannot send weapons to an entity that uses the weapons to carry out serious violations of international humanitarian law such as the 1949 four Geneva Conventions and the 1977 Additional Protocols". He said, so far, many countries had either ignored these provisions or only slightly limited the types of weapons they send. **However, now that the warrants have been issued, those** countries could also possibly be considered to be **complicit in war crimes and crimes against humanity.** "I assume NGOs within the countries will file petitions in the domestic courts to question the legality of continuing to send arms to Israel. **"Even before the ICC decision, Spain and the UK and France limited the weapons they send, but now I think there is a chance that they will have to restrict it further."**

1. **ICC is fine under the constitution**

Human Rights Watch, 350-xx-xx, "," No Publication, https://www.hrw.org/legacy/campaigns/icc/docs/final_nopaper.pdf, Date Accessed: 2025-02-17T14:29:40.953Z //RX

Whether or not so conceptualized, many feel that the **ICC is not** in fact **a** 'foreign **court'** or 'foreign jurisdiction' **as anticipated in** the various **constitutional prohibitions**. When the constitutions prohibited extradition to foreign jurisdictions they clearly contemplated national not international jurisdiction. **An international court which states set up, in accordance with i**nternational **law**, and in which they will fully participate as state parties, from financing it to the appointment and removal of judges, for example, is not comparable to any foreign national court. Just as normal extradition procedures and the concerns that such proceedings seek to protect--being to ensure the fairness of the proceeding and the legitimacy of the charges- **do not apply** to surrender to the ICC, nor should this prohibition on the extradition of a state's own nationals.

2. **1NC Carbonaro is about the right to defense -- the context suggests it's about the 2nd amendment -- not anything to do with US constitution. We read BLUE**

Carbonaro 24 — (Giulia Carbonaro, a Newsweek Reporter based in London, U.K. Her focus is on U.S. and European politics, global affairs and housing, 1-23-2024, "Supreme Court decision sparks Texas independence calls", https://www.newsweek.com/texas-independence-supreme-court-border-ruling-texit-1863124) //doa2-6-2025 + master chen 💁

Newsweek reached out to the White House and Abbott's office for comment by email on Tuesday morning. "As a Texan, I wholeheartedly believe that Texas' only viable option moving forward is to vote on #TEXIT," wrote an X user who calls herself a 9th-generation Texian. "The federal government has all but declared war on **Texas**. We **will not** continue to **tolerate** this **blatant usurpation of** Texas' **sovereignty and Constitutional** right to **defense**," she continued, adding that the state should **invoke its right to "alter, abolish, or reform our government** as we may feel expedient, as guaranteed in Article 1 Section 2 of the **Texas Constitution**." Another X user and resident of the state posted: "Texas has state rights to protect ourselves, its citizens, and our borders when a treasonous federal government tries to use treason to override that. The #TEXIT movement is probably stronger than ever now." The Texas Nationalist Movement (TNM) issued a statement condemning the Supreme Court's ruling, saying it believes "that the federal government has, once again, failed Texas." The **movement** is now **urging** Abbott to **"call an immediate special session to explore Texas independence**." Republican

Representative Clay Higgins of Louisiana also condemned the Supreme Court's ruling, saying that the "Feds are staging a Civil War" and that "Texas should hold its ground." Other social media users on X decried the U.S. judicial system and said it was now time for "Texit," adding that they had lost hope in the federal government. "It's time for Texas to secede and make its own laws. The rest of the red states will join," wrote an account called "state secession." What an independent Texas would look likeRead moreWhat an independent Texas would look like This, in part, reflects what the Texas governor has been saying for the past few years since the launch of "Operation Lone Star" in 2021, a security effort led by the state that added thousands of Texas state troopers and National Guard soldiers along the border with Mexico. According to Abbott, who has repeatedly clashed with the Biden administration over the measures he has promoted to stop migrants from crossing into Texas—including the installation of a floating barrier in the Rio Grande—the state's government is stepping in to fill the gap left by the inaction of the federal government. Despite rising calls for "Texit," the state cannot legally secede from the U.S., as it was established following the Civil War, which saw the victories of the union and Texas rejoining the nation. In the 1869 case Texas v. White, it was decided that individual states could not unilaterally decide to leave the union