## AT: International Law Disad

### No Link---Cyber Ops---2AC

#### No link---non-destructive cyber ops can be “use of force.”

Khatuna Burkadze 18. Fulbright scholar at the MIT Center of International Studies as well as a visiting researcher at Columbia University, Bard College and the Fletcher School of Law and Diplomacy. Graduate of the Fletcher School of Law & Diplomacy, Tufts University. “A Shift in NATO's Article 5 in the Cyber Era”. 42 42 Fletcher F. World Aff. 215 (2018).

The definitions of the use of force and armed attack are not provided in the U.N. Charter. In this regard, in its argument on a case concerning Nicaragua, the International Court of Justice rejected a narrow interpretation of "use of force" that limits the term to the employment of either kinetic force or non-kinetic operations generating comparable effects. The Court held that a state's arming and training of guerrilla forces engaged in hostilities against another state qualified as a use of force, a position that has since become widely accepted.'" The logic of the holding leads to the conclusion that non-destructive cyber operations may amount to a use of force. For example, providing malware to a rebel group and training its members to employ that malware in a destructive manner would seemingly qualify.20

### No Link---Cyber Election Interference---2AC

#### The UN Charter allows self-defense against cyber election interference---sovereignty concerns prove.

Francesco Arreaga, 21. J.D. Candidate @ UC Berkeley, Class of 2021. "Cyber Election Interference and the UN Charter ". BJIL. 4-12-2021. https://www.berkeleyjournalofinternationallaw.com/post/cyber-election-interference-and-the-un-charter

The UN Charter creates a system whereby the Security Council is responsible for resolving international conflict. But what happens when a permanent member of the Security Council that has the power to veto resolutions is the actor engaging in cyber election interference against another nation? This article does not deal with the question of how a nation should respond to election interference via cyberspace; it simply deals with the question of whether a nation can respond to cyber election interference under the UN Charter. The only recourse that a nation has to defend itself under this circumstance is through Article 51 of the UN Charter.

Article 51 states that “[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations.” Some international law scholars construe Article 51 as barring a nation from responding to election interference via cyberspace through self-defense. This blog utilizes Russia’s 2016 cyber election interference in the United States as a case study to argue that a nation should be able to act in self-defense against cyber election interference under Article 51 of the UN Charter.

The UN’s Purpose

Article 1 of the UN Charter outlines the four fundamental purposes of the United Nations. First, maintaining international peace and security; second, developing friendly relations among nations that are grounded in the belief that people must have equal rights and self-determination; third, achieving international cooperation in promoting respect for human rights and fundamental freedoms for all; and fourth, being the center for achieving these common goals.

These four purposes are interconnected and should not be conceived of independently from one another. This is especially true for the first two purposes of the charter because international peace is impossible if one State does not recognize the equal rights and self-determination (political sovereignty) of the people of another State. In other words, international peace exists in conjunction with principles of liberty, equality, and self-determination.

Cyber Election Interference Threatens Political Sovereignty

A U.S. Senate Foreign Relations Committee report details how the Russian government attempted to influence “democracy in the United Kingdom through disinformation, cyber hacking, and corruption.” For example, in the period leading to the Brexit referendum, a Russian organization was “actively posting about Brexit” in an attempt to influence the vote and magnify social discord. In 2017, a Russian cyberespionage group launched phishing attacks against French presidential candidate Emmanuel Macron's campaign. Days before the runoff vote in France’s presidential election, hacked emails from Emmanuel Macron’s campaign were leaked online in an attempt to influence the result of the election.

An indictment by Special Counsel Robert Mueller against several members of Russia’s military intelligence agency describes how, in 2016, Russia “conducted large-scale cyber operations to interfere with the 2016 U.S. Presidential election.” Russian agents hacked into the emails of multiple Hillary Clinton campaign employees, including the campaign chairman. They also infiltrated the computer networks of the Democratic National Committee and Democratic Congressional Campaign Committee to steal emails and documents. Russia also engaged in a targeted information warfare campaign through social media by creating fake social media accounts to instigate Americans to join a flash mob opposing Secretary of State Hillary Clinton’s presidential candidacy. Furthermore, a report by the Senate Intelligence Committee extensively details how Russian operatives specifically targeted African American voters on social media.

The Tallinn Manual on the International Law Applicable to Cyber Operations explains that internal sovereignty includes the “authority of a State to independently decide on its political, social, cultural, economic, and legal order.” Cyber operations that disregard another State’s “exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law.” Russia’s cyberattacks during America’s 2016 presidential election disregarded the UN Charter’s purposes of maintaining international peace or respecting the right of self-determination, and violated America’s internal sovereignty.

Whether a State May Act in Self-Defense when Cyber Election Interference Occurs

One view of cyber election interference is that these acts exist in a “gray zone” of international law. Professor Gary Corn explains how hostile activities in the “gray zone” of international law occur in “the far more uncertain space between war and peace.” They are understood as actions that are aggressive and rise above normal but are “deliberately designed to remain below the threshold of conventional military conflict and open interstate war.” International actors exploit this gray zone in the law because they alter the status quo while not clearly violating international law or starting war.

A second view, that of Professor Michael N. Schmitt, suggests that Russia’s cyber election interference “is not an initiation of an armed conflict” and that, therefore, the U.S. cannot respond in self-defense under the UN Charter. It is “impossible to draw definitive red lines regarding cyber election meddling in the context of the territorial aspect of sovereignty, except with respect to situations causing physical damage or at least a significant impact on functionality.” Scholars also point to how armed attacks are typically those that can cause death.

For example, international law experts who contributed to the Tallinn Manual on International Law Rule 71(5) explain that a critical factor in deciding whether a cyber intrusion is an armed conflict is determining whether the cyber operation is analogous to actions “otherwise qualifying as a kinetic armed attack.” Moreover, the cyber operation must involve the use of a cyber weapon, defined in the Tallinn Manual on International Law Rule 103(2) as “cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack.”

A final view is that a nation may respond in self-defense when facing cyber election interference. President Joe Biden has characterized foreign election interference as a threat to “America’s sovereignty, democratic institutions, and national security.” He has asserted that he “will treat foreign interference in our election as an adversarial act” and make full use of “executive authority to impose substantial and lasting costs on state perpetrators.” These assertions are in line with the long held view in the United States that Article 51 of the UN Charter may be interpreted to mean that the country may act “in self-defense in response to any amount of force by another State.”

A State Must be Able to Act in Self-Defense in the Face of Cyber Election Interference

The creation of cyberspace and the advancement of technology have fundamentally changed the methods nation states may use to violate the sovereignty of other nations or pose threats to international peace. Sovereignty is the first principle outlined in the UN Charter, which declares that the “organization is based on the principle of the sovereign equality of all its Members.” The fourth principle of the United Nations expounds on the importance of sovereignty by establishing that “all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state.” Finally, sovereignty is connected with the U.N. Charter’s second purpose, which is to foster relations among nations based on respect for equal rights and the self-determination of people.

Russia’s interference in the 2016 American presidential election threatened the political integrity and sovereignty of the United States and contradicted the principles and purpose of the UN Charter. Any nation must be allowed to defend itself against such an act of aggression. The United States’ interpretation of Article 51 is the only means of upholding the purposes of the UN Charter, especially when cyberattacks are perpetuated by other members of the UN Security Council that can veto UN Security Council resolutions.

Even if it were the case that cyber election interference were not considered an “armed attack,” Judge Simma noted in his separate opinion for the Oil Platforms case, that a State is able to respond to an attack that does not reach the “armed attack” threshold of Article 51 of the UN Charter. Importantly, the State being attacked may defend itself “within a more limited range and quality of responses…and bound to necessity, proportionality and immediacy in time in a particularly strict way.” This viewpoint is in line with the International Court of Justice opinion in the Nicaragua case that explained how even though one nation’s actions did not rise to the level of an armed attack, the acts could have “justified proportionate counter-measures on the part of the State which had been the victim of these acts.”

Conclusion

A nation must be able to respond to hostile acts by international actors that threaten the soundness of its electoral system. This is not only normatively beneficial but also comports with the UN Charter’s purpose. Our perception of international conflict often does not account for the technological advancements that permit cyberspace to be exploited for harmful means. It is critical that we develop an understanding of international law that accounts for the new challenges we face in world affairs.

### No Link---Response---2AC

#### NATO has been attacked---response is legal.

Franklin D. Kramer et al. 20. Franklin D. Kramer is a distinguished fellow with the Scowcroft Center for Strategy and Security and a board director of the Atlantic Council Lauren M. Speranza is director of Transatlantic Defense and Security at the Center for European Policy Analysis (CEPA). Conor Rodihan is an assistant director in the Scowcroft Center for Strategy and Security’s Transatlantic Security Initiative. "NATO needs continuous responses in cyberspace". Atlantic Council. 12-9-2020. https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/

Customary international law, including the law of countermeasures, pleas of necessity, and other cyber norms, provides the international legal basis for a strategy of persistent engagement. Because NATO Allies have already been attacked and are continuously being targeted by these adversaries, offensive actions to counter such activities are justified, as long as they are conducted proportionately. While persistent engagement arguably could increase instability in cyberspace, Alliance inaction is far more dangerous. If Russia and China perceive no consequences to their malign actions in cyberspace, they will only continue and even intensify them.

### No Modeling/Internal Link---2AC

#### No internal link---states have independent understanding of cyber law---there is no universal norm.

Brandon S. Davis 18. Masters Thesis. “State Cyber Operations and International Law: Russian and Western Approaches.” Graduate Program in Slavic & East European Studies. The Ohio State University. 2018. https://etd.ohiolink.edu/apexprod/rws\_etd/send\_file/send?accession=osu1523531316393533&disposition=inline

It is apparent through this research that the differences in the application of international law to cyber operations among nation-states causes significant issues in international relations. The main consequence is that nations with different applications of international law operate within cyberspace according to their own ideas of permissibility. This causes ambiguity in what constitutes a state of peace or war. Peaceful actions by some may be considered hostile actions by others. Assumptions by US policymakers and strategists that there exists a universal understanding of international law leads to ineffective cyber strategies and miscalculations of an adversary’s actions

### AT: LOAC/Norms Impact---Noncompliance---2AC

#### Law of War is dying now---non-compliance.

Blaise Cathcart 22. Served as the Judge Advocate General (JAG) of the Canadian Armed Forces (CAF) from 2010-2017. "The Creeping Normality of LOAC Noncompliance". Lieber Institute West Point. 4-13-2022. https://lieber.westpoint.edu/creeping-normality-loac-noncompliance/

Taking stock of the state of the Law of Armed Conflict (LOAC) may be one of the most important tasks facing international law today. In that vein, it is well worth asking whether the Law of Armed Conflict is still “fit for purpose”?

As the current conflict in Ukraine illustrates all too well, the answer is not an optimistic one. LOAC increasingly faces an existential challenge. Namely, growing lack of compliance by States and non-State actors (NSAs) threatens its entire legitimacy. Failure of States and NSAs to openly and consistently apply, affirm, and legitimize the fundamental underlying principles of LOAC in today’s armed conflicts will put LOAC into serious disuse. It will profoundly threaten the rule of law and humanity.

### XT---Noncompliance---1AR

#### No one complies now---outweighs the link to the aff.

Blaise Cathcart 22. Served as the Judge Advocate General (JAG) of the Canadian Armed Forces (CAF) from 2010-2017. "The Creeping Normality of LOAC Noncompliance". Lieber Institute West Point. 4-13-2022. https://lieber.westpoint.edu/creeping-normality-loac-noncompliance/

Armed conflict today is massively complex and challenging for States, NSAs, and civil society. The operating environment is multi-domain, hyper-violent, ambiguous, and often blurred. Conflicts are increasingly described as “new wars,” “grey zone wars,” and “hybrid wars.” They are more frequent, more protracted, more influenced by NSAs, more violent, and exponentially more dangerous and deadly for civilian populations. However, from the perspective of LOAC, it appears that these “new wars” or “grey zone wars” present many of the same challenges, albeit more of them, as “old wars” or “black and white zone wars.”

A review of contemporary armed conflicts since the end of the Second World War leads to a somewhat pessimistic view of the effectiveness, credibility, and legitimacy of LOAC. Examining today’s conflicts in Ukraine, Syria, Yemen, Iraq, Afghanistan, Democratic Republic of Congo, Somalia, and South Sudan, and past conflicts in the former Yugoslavia, Chechnya, Rwanda, Columbia, Nicaragua, and Vietnam, the sheer number of gross LOAC breaches and human rights violations, particularly against civilian populations, is shocking and abhorrent. Whether such conflicts are considered international armed conflicts (IACs), non-international armed conflicts (NIACs), or a mix of both, LOAC applies. Every State is a Party to the four Geneva Conventions (GCs) and they are considered reflective of customary international law (CIL) binding on all States.

Yet, in virtually every contemporary conflict, these basic rules—many of which are universally accepted and fundamental rules of humanity—are consistently breached by States and NSAs. The International Committee of the Red Cross (ICRC), along with most States, have acknowledged that noncompliance with LOAC remains an “intractable problem.” To my mind, this problem is the greatest current challenge to the continued credibility of LOAC and there is an “imperative need” to improve compliance.

#### International law norm violation is common---even unrelated fields thump the impact.

Ingrid Wuerth 17. Helen Strong Curry Professor of International Law at Vanderbilt Law School. "Does International Law Have a “Broken Windows” Problem?". Lawfare. https://www.lawfareblog.com/does-international-law-have-broken-windows-problem

Many norms of international law, especially international human rights law, are widely violated. The international legal system as a whole may suffer as result.

International human rights law has changed international law. The two primary sources of international legal obligations—treaties and custom—have become more expansive and looser so as to bring more human rights norms into the ambit of international law, despite wide-spread non-compliance with those norms. In one sense, the success of the effort is clear: international law now regulates a vast array of human-rights-related conduct. Whether the expansion is an effective way to promote human rights is widely-debated.

The broader, unacknowledged problem, however, is the potential effect of the expansion on international law as a whole, as I discuss in detail here. Today, international law includes a broad range of human rights norms which are routinely violated, from the U.N. reporting requirements to gross violations of human dignity. Wide-spread violations of some legal norms may, in turn, make it harder to enforce others. As a (very) imperfect analogy, consider the “broken windows” theory of crime prevention: widespread violations of human rights law may be a symbol of unaccountability, a signal that no one cares about violations of international law and that no one is in charge. Accountability is a fundamental concern of public international law because the system lacks a centralized enforcement mechanism. Whatever the merits of the “broken windows” argument in the context of domestic law enforcement, behavior which signals a lack of accountability may be especially damaging to international law writ large.

Theoretical literature on compliance with international law suggests that non-compliance in some areas makes other norms of international law harder to enforce. Work on rational choice posits, for example, that states comply with international law in part to protect their reputations. If states as a whole tend to expect non-compliance from each other, the costs of entering into treaties or developing norms of customary international law become higher for all states. A baseline reputation of non-compliance among states generally harms interstate cooperation because it means that states will have to do more in a treaty agreement to generate trustworthy commitments (such as monitoring non-compliance), and because it makes some agreements not worth the time or effort. To be sure, these effects depend upon states having reputations for compliance which are not entirely issue-specific or compartmentalized, a plausible assumption for reasons explained here (pages 103-06).

### AT: UN Security Council Impact---2AC

#### UN Security Council can’t solve war.

Hesham Youssef 2/28/22. Jennings Randolph Senior Fellow at USIP. “Here is a way for international law to better help end conflicts.” https://ifit-transitions.org/commentaries/here-is-a-way-for-international-law-to-better-help-end-conflicts/

While the last century’s great wars resulted in setting international rules to regulate conduct during conflicts, and significantly advanced international law (especially IHL), international norms around conflict – and the institutions meant to face them, particularly the UN Security Council – have fallen devastatingly short in resolving conflicts. This trend could deepen in the context of the evolving great-power competition.

A reframing effort of such norms is overdue. The world needs a legal instrument to aim at encouraging and supporting peace negotiations for the peaceful settlement of internal armed conflicts.

The Middle East: Nexus of the World´s Challenges

The Middle East has the dubious distinction of hosting some of the world´s most persistent and dire conflicts and crises. It is home to the Israeli-Palestinian conflict, one of the most enduring struggles. The UN Secretary General declared the situation in Yemen to be the world’s worst humanitarian crisis with 80% of the country’s population in need of humanitarian assistance and protection. Meanwhile, Syria has by far the largest forcibly displaced population worldwide: 6.6 million refugees and more than 6 million internally displaced people, constituting around half the Syrian population. The conflict in Libya is characterised by a weak government, a constellation of militias, and a political class in which many are not only backed by foreign governments but also divided across ideological and tribal lines. Meanwhile, Tunisia, Sudan, Lebanon, Algeria, and Iraq are facing varying degrees of instability and civil strife. The Iranian nuclear file and Iranian policies are also a source of major tension and instability in the region.

Today, not a single conflict in the Middle East is on a solid path towards a political solution. A series of UN peace envoys have come and gone to no avail, while several of the parties involved continue to pay lip service to political settlements but act in a manner more consistent with a military solution. The polarisation witnessed in the region, with different countries supporting opposing parties in conflicts, is making it exceedingly difficult to achieve political settlements.

### XT---UN Fails---1AR

#### UN rules can’t solve peace---empirically fails and great powers have vetoes.

Atanu Biswas 3/30/22. Professor of Statistics, Indian Statistical Institute, Kolkata. "What good is the UN in its present shape". Statesman. 3-30-2022. https://www.thestatesman.com/opinion/good-un-present-shape-1503055779.html

The UN, however, failed utterly – as it was destined to – in instrumenting effective international diplomacy. How worthy is it then to maintain a white elephant like the UN? One may recall that the Nobel Peace Prize for 1988 was awarded to the United Nations Peacekeeping Forces “for preventing armed clashes and creating conditions for negotiations.”

However, the United Nations has failed to prevent war and fulfil peacekeeping duties many times during its history: in Palestine, ever since the creation of the Jewish state in 1948, in Cambodia during the 1970s, in the Somali civil war since 1991, in the Rwandan civil war in 1994, during the Srebrenica Massacre in 1995, during the Darfur conflict in Sudan since 2003, in the Iraq invasion during 2003-11, in the Syrian civil war since 2011, in South Sudan since 2013, in the Yemen civil war since 2014, during the Rohingya crisis in Myanmar since 2017, among others.

On the 20th anniversary of the Rwandan genocide in Kigali, Ban KiMoon admitted that the UN had done a lot to prevent the slaughter of hundreds of thousands of Tutsis but “could have done much more”. Certainly, it could have done more with the Rohingya crisis, in Afghanistan, in the Arab Spring, amid disasters in Haiti, the Philippines, and in many other places. And, of course, there is the classic example of the Security Council’s authorisation of force to turn back Saddam Hussein’s Iraq after its invasion of Kuwait in the early 1990s. Is the 76-year-old UN a toothless and clawless body that no one takes seriously? Is it almost defunct?

António Guterres described Russia’s move (to recognize the so-called ‘independence’ of certain areas of the Donetsk and Luhansk regions) as “a death blow” to the Security Councilendorsed Minsk Agreements, the fragile peace process regulating the conflict in eastern Ukraine. One serious problem of the UN is deeply rooted in the veto power bestowed on the five permanent members. Any of the Big Five can stop any resolution unilaterally.

When the UN was founded in 1945, permanent membership of the Security Council and the veto power ensured that America and the Soviet Union had nothing to worry about – however undemocratic that may sound. Due to this veto power, each of the Big Five could act without any fear of reprisal from the UN. Amnesty International claimed that the five permanent members had used their veto to “promote their political self-interest or geopolitical interest above the interest of protecting civilians”.

### Impact D/Case Turns DA---2AC

#### International law that can’t accommodate CDOs is self-defeating---collapses stability and is terminally unsustainable.

NOTE: CDOs = Cyber Disinformation Operations.

Wenqing Zhao 20. J.D., Yale Law School, 2020; B.A., College of William & Mary, 2017. “Cyber Disinformation Operations (CDOS) and a New Paradigm Of Non-Intervention.” https://jilp.law.ucdavis.edu/issues/volume-27-1/27.1\_ZHAO.pdf

Drawing on the observations on CDOs and existing international laws, I offer the following possible events: (1) current international legal doctrines, including UN Article 2(4)’s “use of force,” the principle of nonintervention, and the prohibition of perfidy, all presume certain levels of aggression and coercion, notions both derived from a narrative of traditional armed conflicts and made to address measures effectuating results similar to those achieved by armed conflicts; (2) technology and cyber capacity have gradually made it unnecessary to effectuate political results through facially aggressive or coercive means on the physical territory of a foreign state; (3) old standards of aggression and coercion consequently become ill-suited to address covert cyber operations, leaving a gap in international law; (4) the twilight zone of international law in turn incentivizes states to exploit the gap and to engage in shady cyber practices like CDOs; (5) during this process, CDOs that are fraudulent and covert greatly undermine interstate trust because of states’ worry of asymmetrical information, which also creates significant inefficiency as states engage in expensive remedial measures of discerning and filtering disinformation; (6) the lack of an international consensus on cyber countermeasures also exacerbates interstate instability as states may adopt over-defensive tactics that are not proportionate in scope; and (7) as technology and cyber capacity continues to advance while international law lags behind, international peace and security will inevitably deteriorate to the point where the current international laws, in refusing to adapt to the changes in cyber space, destroy their own primary objectives of peace-keeping.

Many of these events have already happened, as various reports cited in Section II suggest; the rest are highly likely to happen absent an eventbreaker of international cyber consensus adopting a new paradigm other than “use of force,” coercion, or territoriality. For instance, the proliferation of cross-border CDOs will almost certainly ensue given how cheap, accessible, and innocent CDOs are in comparison to conventional military measures. CDOs will also destabilize inter-state relationships, as they are perceived as threatening yet inconspicuous and un-punishable under current international laws. As I have mentioned, Russia claimed that its CDOs into other states were responding to threats from external cyber informational activities, which are themselves a form of CDOs. The U.S. also put forward several presidential executive orders imposing economic sanctions through OFAC in the event of foreign interference,139 culminating in the most draconian one - Executive Order 13848. This Order, on top of its regular making of SDN, also provides authority to the Secretary of the State and the Secretary of the Treasury to sanction the largest business entities licensed or domiciled in the interfering state in sectors of particular “strategic significance” to that interfering state, regardless of whether or not those business entities have engaged in foreign interference140.

While we previously questioned the effectiveness of economic sanction regimes, as those regimes targeting individuals and entities might be insufficient to deter CDOs, here we have a different worry of over-punishment when no standard of international law can provide guidance on the proper counter responses. Targeting the largest business entities could significantly undercut the economy of the entire sanctioned state, which might seem to many as an unjustified over-response to CDOs. Executive Order 13848 contains an implicit proportionality requirement as “all recommended sanctions shall be appropriately calibrated to the scope of the foreign interference identified,”141 but the standard of proportionality is not discussed and seems to be within the discretion of “appropriate agencies.” Without clearer international laws on CDOs, such discretionary countermeasures would be one of the only few resorts for a state to seek justice.

Even if the prisoner’s dilemma is overstated in the event cascade, and that interstate stability would not be significantly undermined by the lack of international cyber norms, it is still to states’ great benefit to start establishing international cyber norms, to provide deterrence against cyber interference, and to commit to information integrity and cost-effective mechanisms to mitigate the externality of cyber chaos.

### Impact Turn---Nuclear LOAC Bad---2AC

#### Turn---following “law of war” collapses nuclear deterrence AND causes counterforcing and arms racing---each causes nuclear war.

Steve Fetter and Charles Glaser 4/25/22. Steve Fetter is a professor in the School of Public Policy at the University of Maryland. Charles Glaser is professor of political science and international affairs and director of the Institute for Security and Conflict Studies at the Elliott School of International Affairs. Legal, but Lethal: The Law of Armed Conflict and US Nuclear Strategy, The Washington Quarterly, 45:1, 25-37, https://cpb-us-e1.wpmucdn.com/blogs.gwu.edu/dist/1/2181/files/2019/03/FetterGlaser\_45-1\_TWQ.pdf

Although abiding by the LOAC might appear to be a clearly good idea—better to be legal than illegal—we should not assume that it provides good guidance for US nuclear strategy and, in turn, US national security policy. Instead, we need to consider the implications of the LOAC for the probability of a nuclear war and the damage that would result if war occurs. In particular, we need to consider the impact on deterrence and crisis stability, and on incentives for escalation and arms racing. Our analysis finds that the LOAC provides dangerous guidance across multiple dimensions of nuclear strategy.

First, depending on one’s understanding of the LOAC, the required strategy would leave the United States with an inadequate deterrent when facing certain types of adversaries. Second, and more importantly, the counterforce strategies that are legal under the LOAC would in practice (if not necessarily in theory) help to preserve and reinforce the long-standing US emphasis on counterforce targeting, including supporting improvements in its large and sophisticated counterforce arsenal. US nuclear doctrine includes a spectrum of counterforce options—ranging from limited attacks intended to deter conventional war and nuclear escalation to full-scale attacks against nuclear forces, command and control, and leadership that are designed to reduce the damage the adversary can inflict against the United States and its allies.

The problem is that a counterforce doctrine is not the United States’ best option for dealing with opposing states that have deployed large capable arsenals, which make significant damage-limitation essentially infeasible. Under these conditions, a doctrine that targets civilians and the infrastructure that is necessary for their survival (“countervalue attacks” in the terminology of nuclear strategy)9 avoids a variety of dangers, including: incentives to launch a massive counterforce attack during a severe crisis or conventional war, which undermines crisis stability; and intensified arms competition with the United States’ majorpower nuclear competitors, Russia and China, which unnecessarily strains political relations and increases the probability of conflict. In addition, a countervalue strategy that includes a spectrum of options, ranging from small attacks against isolated infrastructure targets to large attacks against civilians, is the deterrent strategy that flows logically from the defining feature of nuclear weapons— their ability to inflict enormous damage. The increasing acceptance and legitimacy of the LOAC within the US government works to preserve the US counterforce strategy by adding another influential argument opposing the coercive countervalue logic of nuclear weapons.

Before jumping into this analysis, we raise a couple of reasons for skepticism about applying the LOAC to nuclear strategy. The LOAC is not designed to deal with the core challenge posed by nuclear weapons—how to avoid nuclear war. The LOAC was developed over centuries of armed conflict and was formalized in the 1864 Geneva Convention as well as the 1899 and 1907 Hague Conventions. It governs the conduct of forces when engaged in armed conflict (jus in bello), but neither the decision to go war (jus ad bellum), nor the preparation for deterring or fighting a war. The purpose of the LOAC is to not to deter or prevent war, but rather to moderate the conduct of armed conflict and to mitigate the suffering it causes.10 The premise is that war will occur, but that the horrors of war can be limited through applying certain legal and ethical principles.

This would appear to make the LOAC less relevant to nuclear strategy, for which the primary goal is to prevent nuclear war in the first place. The horrors of nuclear war can be limited primarily by deterring the use of nuclear weapons in the first place—and, if deterrence fails, by limiting escalation to large-scale attacks. We should not simply assume that legal and ethical principles that were developed to moderate the conduct of conventional conflicts would be optimal or even suitable for deterring nuclear war and limiting escalation. Additional skepticism is due because the logic of nuclear strategy differs dramatically from the logic of conventional strategy.11

### XT---Nuclear LOAC Bad---1AR

#### Nuclear LOAC collapses deterrence, crisis stability, and relations---makes nuclear conflict more likely.

Steve Fetter and Charles Glaser 4/25/22. Steve Fetter is a professor in the School of Public Policy at the University of Maryland. Charles Glaser is professor of political science and international affairs and director of the Institute for Security and Conflict Studies at the Elliott School of International Affairs. Legal, but Lethal: The Law of Armed Conflict and US Nuclear Strategy, The Washington Quarterly, 45:1, 25-37, https://cpb-us-e1.wpmucdn.com/blogs.gwu.edu/dist/1/2181/files/2019/03/FetterGlaser\_45-1\_TWQ.pdf

More important than the deterrence problem is the counterforce problem. The targeting policies allowed by the LOAC lend support to dangerous US force structures and nuclear strategies. This counterforce/damage-limitation emphasis generates a variety of well-known dangers, especially when facing another major nuclear power, including reducing crisis stability—creating both real and exaggerated incentives to launch preemptive attacks—and fueling military competition and straining political relations.18 In other words, an LOAC-compliant US nuclear strategy would not just limit the US ability to deter nuclear conflict, but by allowing large-scale counterforce targeting, the LOAC allows a strategy that makes nuclear conflict more likely through accident, miscalculation, or preemption in a crisis, and makes crises themselves more likely by damaging US relations with its major-power adversaries.

The problem we see is that in practice the LOAC will (and already does) lend significant support to US pursuit of large, sophisticated counterforce/damagelimitation forces. US nuclear strategy has a long history of emphasizing large counterforce missions, including pursuit of a damage-limitation capability against the Soviet Union during the Cold War,19 and the United States has been unwilling to foreswear the pursuit of a damage-limitation capability against China’s growing nuclear force.20 During the Cold War, the United States offered a variety of weak arguments to explain and justify the acquisition of large counterforce forces. These included deterring additional limited nuclear attacks, protecting one’s own forces from additional attacks, ensuring that the adversary could not gain an advantage in a counterforce exchange, and threatening nuclear forces because the adversary places great value on them.21 Still more worrisome, the United States pursued damage-limitation for decades even when its prospects were clearly poor.22 Even though many of these specific arguments have had reduced currency since the end of the Cold War, the US commitment to counterforce continues and much of this is driven by pursuit of damage-limitation capabilities. Especially given the development of technologies that increase the prospects for making mobile forces vulnerable,23 it is likely that the United States will continue to pursue the ability to destroy all of China’s forces, and possibly Russia’s.

The LOAC support this outcome by presenting a simple and appealing conclusion that proponents of counterforce forces can employ in support of their preferred strategy: with countervalue targets prohibited, all that is left is counterforce; and if attacking opposing forces is all that is permitted, the United States should do this as effectively as possible. Doing anything less would leave the United States with a weakened and possibly ineffective deterrent. Consequently, although a nuanced understanding of the LOAC prohibits damage-limitation counterforce attacks against states with truly massive retaliatory capabilities, the United States is likely to ignore this constraint when policy and plans are being made. The result is that the LOAC lends support to a dangerous US nuclear strategy.

During the Obama administration, retention of substantial counterforce capabilities was justified partly by the requirement that all plans must be “consistent with the fundamental principles of the Law of Armed Conflict.” 24 US nuclear planners embraced the LOAC as justification for the pursuit of counterforce and damage-limitation capabilities, especially because the LOAC is interpreted to impose a strict ban on countervalue retaliation. They rejected reductions to “minimum deterrent” force levels partly because the countervalue targeting that would be required for a small nuclear force to be an effective deterrent would be incompatible with the LOAC. The LOAC is therefore a barrier to deep reductions in nuclear arsenals, which is ironic for those who believe LOAC compliance can be achieved only through a prohibition on nuclear weapons and who see deep reductions as an essential waystation on the path toward nuclear disarmament.

#### We control the probability and magnitude of impacts

Steve Fetter and Charles Glaser 4/25/22. Steve Fetter is a professor in the School of Public Policy at the University of Maryland. Charles Glaser is professor of political science and international affairs and director of the Institute for Security and Conflict Studies at the Elliott School of International Affairs. Legal, but Lethal: The Law of Armed Conflict and US Nuclear Strategy, The Washington Quarterly, 45:1, 25-37, https://cpb-us-e1.wpmucdn.com/blogs.gwu.edu/dist/1/2181/files/2019/03/FetterGlaser\_45-1\_TWQ.pdf

Preventing Nuclear War Should Guide Nuclear Strategy

In sum, we believe that the LOAC provides poor guidance for US nuclear policy. Although intuitively appealing—because attacking civilians would be horrible— this appeal is misleading. Nuclear policies guided by the LOAC risk leaving the United States without an adequate deterrent and, more importantly, support force postures that make both nuclear war and escalation to all-out war more likely. Moreover, a nuclear war driven by the pressures created by large counterforce forces would likely inflict the very huge costs to civilians that abiding by the LOAC seeks to avoid.

So long as the United States retains nuclear weapons, it should rely on a strategy that meets its deterrence requirements while minimizing incentives and pressures for nuclear use during crises, the probability of accidents and unauthorized use, and strains in political relations that are generated by arms races. In addition, if deterrence fails, the strategy should create incentives for the slow and deliberate use of nuclear weapons, not impulsive, rapid, or massive attacks. This can be achieved by a countervalue strategy that includes a range of limited nuclear options and little or no counterforce capability. The United States could adopt this policy unilaterally, but cooperation with major-power nuclear adversaries would increase both the prospects for and effectiveness of this policy. Arms control agreements that constrain counterforce forces, thereby reducing incentives to attack early and massively, would reduce the probability of nuclear war and, if desirable, pave the way to reductions in the size of states’ forces. This type of agreement would also reduce the danger posed by the targeting allowed by the LOAC, although the logic for targeting nuclear forces would remain weak.

The LOAC misguides US nuclear policy. The most ethical and moral nuclear policy is the one that minimizes the probability of nuclear war and the probability as well as extent of escalation if nuclear war does occur. This strategy is precluded by the law of armed conflict.