## International Law Disad

### OFF

#### Information warfare is not an armed attack---the plan’s definition of cyber thresholds lowers the line for breaking international law.

Ryan Goodman 17. Co-editor-in-chief of Just Security and Anne and Joel Ehrenkranz Professor of Law at New York University School of Law. "International Law and the US Response to Russian Election Interference". Just Security. 1-5-2017. https://www.justsecurity.org/35999/international-law-response-russian-election-interference/

On Thursday, Senator McCain will hold hearings of the Armed Services Committee on the Russian election hacking. Several aspects of Russia’s election interference raise issues involving the international law of cyber operations. For a quick tutorial, I recommend most highly an earlier Just Security post by Sean Watts, “International Law and Proposed U.S. Responses to the D.N.C. Hack.” I thought to provide readers with a few additional points in light of more recent developments.

1. Were the Russian operations an “act of war,” as Senator McCain recently stated?

Short answer: No, none of the facts alleged by the Obama administration with respect to the Russian operations would amount to an “act of war” in any legal sense of what that term might mean. And, yes there is a fairly settled understanding of what constitutes such actions in cyber.

Longer answer: An “act of war” is, in this context, a misplaced term. Sen. McCain’s statement likely intended to refer to an “armed attack” under modern law on the resort to force including the UN Charter. To cross the threshold of an armed attack, the cyber operations must at the very least involve a “use of force.” In an important speech in 2012, then-State Department Legal Adviser Harold Koh explained the US view of when cyber operations involve the use of force: “Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.” That view is widely accepted by international legal experts (see posts by Mike Schmitt in the context of the Sony Hack and by Sean Watts in the context of the DNC hack, explaining the consensus view.) And as Sean Watts explained in his analysis, “it is enormously difficult to imagine a persuasive characterization of the D.N.C. hacks as either uses of force or armed attacks.”

One caveat: Technically speaking (and international law, to be sure, can be hyper technical), Koh’s remarks do not place a lower limit on what constitutes a use of force in cyber. Or another way of putting that point: his remarks do not state that such effects—“death, injury, or significant destruction”—are a necessary condition for a cyber act to constitute a use of force. Illustrating the point that a use of force need not itself be destructive, in a case between the United States and Nicaragua, the International Court of Justice characterized “arming and training” rebels as “involving the use of force.” (para. 228) That said, for a lookback at historical US resistance to a broader conception of “armed attack,” I recommend Matt Waxman’s “Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)” in the Yale Journal of International Law in 2011 (especially pages 427-30 & 437-40).

2. Has the Obama administration called the Russian operations a violation of international law?

Short answer: No.

Longer answer: All official statements by the Obama administration appear to include a studied avoidance of whether the Russian actions do or do not violate international law. Note this conspicuous line in the President’s statement on December 29: “These actions … are a necessary and appropriate response to efforts to harm U.S. interests in violation of established international norms of behavior.” Political scientists talk about “international norms of behavior”—for international lawyers, on the other hand, such terms do not connote an international legal obligation. It is safe to assume the specific word choice in the President’s statement is highly deliberate.

The administration had another opportunity recently to label action like the Russian DNC hack a violation of international law, but didn’t. In November, the State Department’s Legal Adviser Brian Egan gave an important speech on cyber and international law. In discussing this area of law, his description of cyber activities that would violate a State’s international obligations would not match the hacking of the DNC. He said:

“For example, a cyber operation by a State that interferes with another country’s ability to hold an election or that manipulates another country’s election results would be a clear violation of the rule of non-intervention.” (emphasis added)

Two caveats: First, as with Koh’s speech, the Egan speech does not set the outer limits of what action would violate the relevant legal rule. It only gives two examples of “clear” violations. Second, one of the two examples—a cyber operation “that manipulates another country’s election results”—might apply to hacking of election facilities (e.g., voting booths), of which Russians have also been accused. I suppose the legal question may boil down to whether an operation intended to cast grave public doubt on the integrity of the results would count, or if the Egan speech is meant instead to refer to altering the actual outcome.

3. Why would the Obama administration not say whether the Russian actions do or do not violate international law?

Short answer: There could be multiple different explanations.

Longer answer: Perhaps the administration lawyers did not reach a consensus view on whether the actions violated international law. Perhaps the administration reached the view that the Russian actions do not amount to such a legal violation, and so did not say otherwise. Perhaps the administration does think the Russian actions amount to a legal violation, but there is no pressing reason to state it. Or perhaps the administration is reluctant to assume the role of a victim, and consequent appearances of weakness or vulnerability, in its international relations with a recently resurgent Russia?

Also, talking about the law would open up questions about when, if ever, U.S. cyber operations violate international law.

4. What is at stake in the question whether the Russian actions violate international law?

There is no short answer.

First, if the Russian actions violated international law, it could expand the scope of actions the United States could take in response. Under the international law on “countermeasures,” the United States would be permitted to engage in self-help measures that would themselves otherwise violate international law. That is, a State is permitted to break international law to stop another State from breaking international law, in some circumstances. (There are conditions placed on the exercise of such measures, which I do not delve into here.)

#### NATO’s cyber collective defense sets a legal framework for the concept of armed attack.

Michael Schmitt 2/24/22. Professor of International Law at the University of Reading in the United Kingdom; G. Norman Lieber Distinguished Scholar at the U.S. Military Academy at West Point; Strauss Center Distinguished Scholar and Visiting Professor of Law at the University of Texas; professor emeritus at the U.S. Naval War College; and Director of Legal Affairs for Cyber Law International. He serves on the Department of State’s Advisory Committee on International Law, is a member of the Council on Foreign Relations and a Fellow of the Royal Society of Arts, and is General Editor of The Lieber Studies (OUP). "Expert Backgrounder: NATO Response Options to Potential Russia Cyber Attacks". Just Security. 2-24-2022. https://www.justsecurity.org/80347/expert-backgrounder-nato-response-options-to-potential-russia-cyber-attacks/

Over recent weeks, concern has been expressed that Russia might launch hostile cyber operations against the United States and other NATO members in parallel with a military campaign against Ukraine. That military campaign is now fully underway. This article examines how the feared Russian cyber operations would be characterized under international law and outlines the response options open to States targeted by them. The analysis is, among other things, a cautionary note to those who would too readily jump to describing such Russian operations as an “attack” that triggers the alliance’s collective self-defense mechanism. It is important to sort through the more likely scenarios of Russian-led activity below that threshold, as well as if that threshold is crossed. And it’s important to comprehend how the legal framework applies to Russian use of non-state actors to carry out such operations. All this and more in the analysis that follows.

#### That destabilizes international law---allows early use of force.

Michael Schmitt 14. Professor of International Law at the University of Reading in the United Kingdom; G. Norman Lieber Distinguished Scholar at the U.S. Military Academy at West Point; Strauss Center Distinguished Scholar and Visiting Professor of Law at the University of Texas; professor emeritus at the U.S. Naval War College; and Director of Legal Affairs for Cyber Law International. He serves on the Department of State’s Advisory Committee on International Law, is a member of the Council on Foreign Relations and a Fellow of the Royal Society of Arts, and is General Editor of The Lieber Studies (OUP). "International Law and Cyber Attacks: Sony v. North Korea". Just Security. 12-17-2014. https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/

Pursuant to Article 51 of the UN Charter and customary international law, if the malicious cyber operation against Sony had constituted a “use of force” rising to the level of an “armed attack,” the United States would have been entitled to respond forcefully, whether by kinetic or cyber means. The IGE unanimously agreed that cyber operations alone may be sufficient to cross the armed attack threshold, particularly when they cause substantial injury or physical damage. Some members of the group went further by focusing not on the nature of the harm caused, but rather its severity. In their view, a sufficiently severe non-injurious or destructive cyber operation, such as that resulting in a State’s economic collapse, can qualify as an armed attack.

The cyber operation against Sony involved the release of sensitive information and the destruction of data. In some cases, the loss of the data prevented the affected computers from rebooting properly. Albeit highly disruptive and costly, such effects are not at the level most experts would consider an armed attack. Additionally, some States and scholars reject the view that the right of self-defense extends to attacks by non-State actors. Even though the attribution of the Sony incident to North Korea has been questioned, this debate is irrelevant because the operation failed to qualify as an armed attack in the first place.

But was the operation nevertheless a violation of Article 2(4) of the UN Charter and customary international law’s prohibition on the use of force by States such that it opened the door to responses other than forceful ones? The prevailing view in international law is that “use of force” is a lower threshold than “armed attack;” all armed attacks are uses of force, but the reverse is not true. Unfortunately, after three years of discussion, the IGE could arrive at no black letter definition of a cyber use of force. Its members merely agreed that States would make case-by-case assessments of non-injurious or destructive cyber operations, considering such factors as severity, immediacy of effect, invasiveness, military character, and so forth.

Although the use of force threshold remains ambiguous, it seems highly unlikely that the international community will characterize operations like that against Sony as such. This hesitancy will be driven in part by concern over the U.S. position (a distinctly minority one) that all uses of force are also armed attacks that allow forceful responses. Some States view the premise as potentially destabilizing in that it allows for an earlier use of force than would otherwise be the case. They will accordingly be extremely reticent about characterizing cyber operations as having crossed that threshold.

#### Destabilizing international law collapses the Long Peace---lowering the UN threshold causes revisionist leaders to selectively apply laws and escalate.

Ingrid Wuerth 17. Helen Strong Curry Professor of International Law at Vanderbilt Law School. "Using International Law to Prevent Interstate War: How Syrian Airstrikes Make the World Less Safe". Lawfare. https://www.lawfareblog.com/using-international-law-prevent-interstate-war-how-syrian-airstrikes-make-world-less-safe

War is in the air: figuratively and literally. Even before the air strikes in Syria and the Russian veto of U.N. Security Council Resolution condemning Syrian use of chemical weapons, President Trump’s unpredictable and combative approach to foreign policy suggested a variety of paths which could lead to armed conflict with Iran, China, Russia or North Korea as Niall Ferguson, Robert Kagan, and Fareed Zakaria have all argued. In the post-World War II period, international law helped generate conditions which led to interstate peace—the “long peace.” Syrian airstrikes have, however, put unprecedented stress on the U.N. Charter-based international legal system regulating the use of force. Perhaps the result will be a more nuanced and better international legal system, one which is carefully calibrated to permit the use of force in response to humanitarian atrocities, as argued by Harold Koh and Rebecca Ingber. But perhaps degradation of the U.N. Charter-based limitations will weaken the international law prohibitions on the use of force, making regional or global conflict with China, North Korea, and Russia more likely. Those proposing an erosion of the U.N. Charter system need to consider carefully whether the international legal system is strong enough to make nuanced use-of-force distinctions. The answer depends in part on politics.

Viewed through a political lens, the prospects for a nuanced and effective international legal prohibition on the use of force look dim. Relaxing the prohibition on the use of force is likely to embolden the territorial ambitions of Russia and China; it will undermine the strength of the U.N. Security Council; and it is especially difficult to administer in a world of fake news and hair-trigger decision-making. The Syrian atrocities cry out for a response, but now is a dangerous time to tinker with the U.N. Charter’s prohibition on the use of force.

It bears emphasizing that for almost a century, the prevention of interstate conflict has been the core objective of international law. The League of Nations, established in the aftermath of World War II was designed to manage great power politics but failed to prevent World War II. That failure was shared by the 1928 Kellogg-Briand pact which outlawed war for the first time. After World War II, the victorious powers created the U.N. Charter and the Security Council with its permanent veto-wielding members: China, France, Russia, United Kingdom, United States. Note the continuing importance of those five powers. The Charter ushered in a remarkable “Long Peace”—meaning a dramatic reduction in inter-state armed conflict. The cornerstone of the U.N. Charter and of the international legal order since 1945 is a prohibition on use of force except in self-defense or as authorized by the Security Council. The “Long Peace” suggests that it has worked: not to prevent all conflicts, but to prevent many inter-state conflicts, which is the type of conflict building now.

Using the Syrian airstrikes to craft a humanitarian exception to the prohibition on the use of force puts the “Long Peace” under unprecedented stress. To be sure, the 1999 NATO bombing of Kosovo for humanitarian purposes violated Article 2(4) of the U.N. Charter. But the Syrian airstrikes, which involved the U.S. acting alone and without exhausting the avenues for peaceful resolution of the issue, represents a significant expansion of the Kosovo precedent, as analyzed by Ashley Deeks here.

There are several reasons to think that a limited and fine-tuned humanitarian exception to the prohibition on the use of force will not work. First, it will embolden the already emboldened territorial aspirations of Russia and China. After the bombing campaign and with the strong support of Western European countries and the United States, Kosovo declared its independence from Serbia in 2008. Serbia and its allies, especially Russia, strongly condemned the declaration of independence and continue today to refuse to recognize Kosovo. Russian officials, then, in turn used the Kosovo precedent to support its use of force in both Georgia and Ukraine. Crimea, which was part of Ukraine, is today Russian. The core threat to peace with Russia is probably—Syria notwithstanding—the increasingly militarized borders between NATO (or NATO-allied) countries and Russia, which includes thousands of NATO troops, the most since the end of the Cold War. The South China Sea is probably the world’s leading conflict-prone area—China’s territorial ambitions there may explain its uncharacteristic reluctance to criticize U.S. airstrikes in Syria. These political facts should give pause to those who seek a carefully-calibrated prohibition on the use of force.

Second, Syrian airstrikes undermine the United Nations Security Council, which did not authorize them, either ex ante or ex post. But the Security Council is a key forum for resolving other threats to interstate peace, such as Iran and North Korea. China, which is widely viewed as the key to containing North Korea, has recently highlighted its participation in developing the U.N. Security Council Resolutions designed to deter North Korean nuclear and missile programs. After all, international law provides the basis for imposing sanctions on North Korea to limit its nuclear ambitions. International law serves core North Korean objectives, too, as it prevents Western military intervention, a fear motivating North Korean policy. The Syrian precedent gives North Korea reason to worry that the U.S. will attack even over a Chinese veto in the Security Council. As with North Korea, international law strongly supports U.S. policy objectives of preventing a nuclear-armed Iran. Sanctions imposed by the United Nations Security Council led to the 2015 Joint Comprehensive Plan of Action, which relaxed sanctions in return for Iranian concessions on its nuclear program. Undermining the U.N. Security Council makes peace more difficult to achieve in this context, too.

Third, President Trump’s destabilizing leadership is the immediate cause of many dire scenarios forecasting war; such leadership makes exceptions to Article 2(4) especially dangerous and especially difficult to limit. President Trump’s use of force in Syria illustrates how hard it is to categorize such interventions as “one-off” incidents (on this point, see the exchange between Monica Hakimi and Anthea Roberts over at EJIL:Talk!) or to define their precedential impact in narrow terms. The very factors that were supposed to limit the Kosovo precedent, including the participation of a regional security organization such as NATO, failed to constrain the primary architect of those very limitations: the United States itself. A nuanced and fine-tuned set of factors justifying the use of force is hard to administer in a world of trigger-happy, truth-challenged leaders.

### Turns Case---2NC

#### Norms turn and outweigh deterrence.

James A. Lewis 09. Center for Strategic and International Studies. The “Korean” Cyber Attacks and Their Implications for Cyber Conflict. October 2009. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy\_files/files/publication/091023\_Korean\_Cyber\_Attacks\_and\_Their\_Implications\_for\_Cyber\_Conflict.pdf

One question to consider is whether we have been too quick to strip cyber conflict from its political context. Given the limitations of deterrence, a nation like the United States, which is uniquely vulnerable, would gain more by creating international norms. These actions would change the deterrent calculus (by reducing the likelihood of success for an opponent in launching a cyber attack and by increasing the cost of being caught) in ways that that are not achievable by threatening reprisal or retaliation.

### UQ---“Use of Force” Limited---2NC

#### Use of force law is limited to physical attacks now---including cyber flips the US position and expands legality of self-defense across the board.

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

Scholars have attempted to update the use of force paradigm to account for emerging cyber operations like CDOs. However, Article 2(4) seems ill-suited as a solution to CDOs. The “use of force” in Article 2(4) has long been read as containing physical violence or resulting in physical harm. This is distinct from other forms of coercion that generally fall under the customary international norm of non-intervention; such interpretation also represents the longstanding position of the U.S.53 There were also significant historical debates over whether or not to clearly define the term “use of force.” One such contention took place in the preparation of UN General Assembly Resolution 2625, the Declaration on Principles of International Law Friendly Relations and Co-operation among States adopted in 1970.54 The Report of the Special Committee on Resolution 262555 unfolded the debate over the definition of “force” in detail. Multiple states had jointly proposed to insert a broad definition of the term “force” in Resolution 2625, such that “force” would include not only military force, but also “all forms of pressure, including those of a political and economic character, which have the effect of threatening the territorial integrity or political independence of any state.”56 Some suggested that forms of pressure exercised on ideological and religious grounds should thus be prohibited.57

However, no agreement was reached by members to either include a definition of “force” in the Resolution 2625 statement or to expand “use of force” to cover any form of pressure against the political independence or territorial integrity of a state. Some representatives would only understand the term “force” to mean exclusively “armed force.” 58 Consequently, no definition of “force” was provided in the Declaration on Friendly Relations. The standard for non-belligerent inter-state actions was instead provided in the principle of non-intervention, a principle that I will further discuss.

In any case, in spite of the fact that ambiguity remains in whether pressure exercised through cyber means could amount to “use of force,” it is unlikely that General Assembly members would agree on elevating cyber meddling to the status of “use of force.” Article 2(4)’s prohibition against “use of force” has so far been a standard of physical violence, not contemplating actions that are short of military natures. To re-propose the expanded definition of “use of force” to cover CDOs is currently unattainable, given that the extended definition would result in significant and unwanted ramifications on the legality of other forms of economic and political pressures, and on the rights of self-defense and countermeasures.

### Link---CDOs---2NC

#### The plan expands “use of force” laws in the UN---allows disproportionate military response.

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

A. Victim States of CDOs Have No Legal Recourse in the United Nations Charter Article 2(4)

The lawfulness of resorting to military measures, the jus ad bellum, is regulated by the Charter of United Nations Article 2(4). Article 2(4) provides 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.”48 No definitions are provided in the Charter, however, for the key terms, “use of force” and “political independence,” except for a mentioning in the preamble that one purpose of the Charter is to “ensure…that armed force shall not be used, save in the common interest.”49 It is altogether unclear if “use of force” in Article 2(4) implies a use of armed force, and it would be imprudent to draw such a definite conclusion as arguments were made that use of force is “a large category of activities containing a smaller subset of events that qualify as armed subset.”50

CDOs, while capable of asserting broad influence on the target states, can hardly fall under the category of armed force. Furthermore, a CDO rarely amount to a “use of force,” even when the term arguably covers operations less grave than armed force. Regardless of the scope of use of force, incursions into a nation’s political independence in the form of CDOs have an “ostensibly peaceful” façade that is non-belligerent in nature, and therefore are “seldom broadly accepted as uses of force.”51 The worry of counting CDOs as “use of force,” other than it is counter-intuitive to the plain language, is that the effect of CDOs might be disproportionate to that of belligerent military actions (the traditional understanding of “use of force”). Consequently, counting CDOs as “use of force” might trigger a state’s countermeasures disproportionate to what CDOs deserve, in forms of draconian economic sanctions or even military actions, especially when the effect of CDOs is extremely hard to measure as I will discuss in later sections.

### Link---“Cyber Ops”---2NC

#### Most cyber operations are below the threshold.

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

Western scholars generally classify cyber operations as a use of armed force if the attack directly or indirectly results in damage to physical property or causes injury or loss of life (Harrison Dinniss 74). In instances where the operation does not clearly cause physical damage, injury, or loss of life, the IGE provides eight criteria to determine if a cyber operation has reached the threshold of “use of force.” These criteria include severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality (Schmitt 334-36). The elements must be taken as a collection of circumstances for a state to make a determination on use of force.

Most cyber operations fall below the use of force threshold. However, Operation Olympic Games is clearly determined to meet the use of force threshold. The US operation continuously caused physical damage to Iran’s infrastructure over a period of years. This is a clear violation of UN Charter, Article 2(4). However, in order for Iran to maintain the legal right to self-defense, the operation would have to classify as an “armed attack”

### Link---Election Hacking---2NC

#### The plan violates international law---you can’t respond to election hacking as an armed attack.

Alex Xiao 20. J.D. Candidate at Duke University School of Law, Class of 2020. “Responding to Election Meddling in The Cyberspace: An International Law Case Study on The Russian Interference in The 2016 Presidential Election”. Duke Journal of Comparative & International Law. Vol. 30:349. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1565&context=djcil

The Russian election meddling operation cannot be categorized as an armed attack under the framework of Tallinn Manual 2.0 because no physical damages were inflicted on persons or objects. This operation is a much weaker case under the current international law framework than that of the Stuxnet operation, where physical property––thousands of Iranian centrifuges––was damaged and disabled.59 If the Tallinn Manual 2.0 experts could not reach a consensus on whether Stuxnet qualified as an armed attack, the DNC hack is even more unlikely to be considered as such.

The “scale and effects” analysis is even more unlikely to qualify the DNC hack as an armed attack.60 Although the Mueller investigation and indictments against Russian individuals have provided much more information, the actual effects of the hack are still almost unmeasurable.61 The way that the Russian election interference operated in influencing the information environment––essentially spreading narratives and messages that were false but also subscribed to by certain American groups, such as the subscribers of Infowars––made it hard for analysts to figure out (1) which parts of the information environment before the 2016 election was created by Russian trolls and (2) which parts originated in the United States.

Categorizing the Russian DNC hack as an armed attack might also invite an escalation of cyber conflict by triggering Article 5 of the North Atlantic Treaty Organization (“NATO”) Charter,62 which calls for a collective response from all NATO States. It could alienate NATO partners to put the entirety of NATO in a confrontation with Russia over an election meddling operation that caused no physical damage. After all, Estonia, even after suffering a much stronger attack from Russia in 2007 that temporarily disabled a large percentage of its Internet system, did not invoke Chapter 5 for these considerations.63

Under Tallinn Manual 2.0 standards, the DNC attack is also unlikely to qualify as a use of force for two reasons. First, on its face, the Russian operation is closer to “non-destructive cyber psychological operations intended solely to undermine confidence in a government,”64 which does not constitute a use of force, than the Stuxnet operation, which, again caused damages on a large amount of State property.

Second, the “scale and effect” factors drawn from Tallinn Manual 2.0 also support the same conclusion that the Russian operation does not constitute a use of force:

1. Severity: Weak. No harm or damages were inflicted on people or property.

2. Immediacy: Strong. The effects of the DNC hack were immediately felt by the United States electorate in a heated election.

3. Directness: Strong. Although the actual effects of the DNC hack are extremely hard to quantify, one can certainly argue that the DNC emails disclosed after the hack directly influenced certain voters’ behaviors in the 2016 elections.

4. Invasiveness: Weak. No target in this operation is a protected or classified system by the United States government. The DNC is a private organization and it uses its servers to promote the mission of the Democratic Party. The Russians never attacked the voting system itself or any government entities related to the election.

5. Measurability of effects: Weak. We are able to measure how much information the Russians stole. However, no data or servers were actually corrupted or damaged. The Russians selectively disseminated the information they gathered for political gain without using physically destructive means. Collecting information, despite via illegal means under United States domestic law, does not by itself violate international law.65

6. Military character: Strong. The Central Intelligence Agency and the Federal Bureau of Investigation found with a high degree of confidence that Russian military intelligence units were behind the operation.66 The GRU hacked into the personal email accounts of Democratic Party officials and distributed the information gathered.

7. State involvement: Strong. For the same reason mentioned above, State involvement is extremely close to this operation. The attack did not come from a private organization supported by the Russian government, but from the military intelligence agency itself.

8. Presumptive legality: Unclear. International law does not provide an answer on this question because scholars are still arguing whether what the Russians did during the 2016 Election was a psychological operation through cyber espionage, which is legal under international law, or something more severe.67 This factor would not help us answer the question of whether the Russian operation constitutes a use of force because, in this case, the characterization of the Russian operation is the most important question that needs to be answered.

Although some of the Tallinn Manual 2.0 factors seem to support categorizing the Russian Hack as a use of force, the most important factor in the analysis––the severity of the effects caused by the cyber operation––does not. The non-violent nature of the operation makes a use of force categorization extremely difficult. Being able to attribute a cyber operation that had certain unquantifiable effects on the 2016 elections to the Russian government does not seem to raise the operation to the level of a use of force because it would not effectively distinguish this operation from other lower level offenses under international law, such as prohibited intervention, which will be discussed in later parts of this Article.

One way to increase the severity of the effects of the Russian operation as a matter of law would be categorizing the election system as “critical infrastructures”68 and treating meddling with the elections akin to tampering with a major dam or an electrical grid. However, the DNC servers are not related to the election itself, but are instead used to promote the interest of a private organization, the Democratic Party. Therefore, even if the election system is categorized as a critical infrastructure as a matter of law, Congress must go the extra mile to consider ways to protect private entities like the DNC to respond to cyber operations like the DNC hack in the future. Either way, classifying the election system as critical infrastructure was unavailable for both the Obama and the Trump Administrations because such classification was not in place before the Russian operation.

Self-defense would not have been a measure available to the United States to respond to the Russian DNC hack in 2016. This is because the operation amounts to neither an armed attack nor a use of force under customary international law, as reflected in Tallinn Manual 2.0. The Russian operation, however, could have been categorized as violating other aspects of international law, to which the United States may respond by either invoking the plea of necessity69 or imposing countermeasures.70 I will next discuss the legal requirements and the applicability of invoking the plea of necessity.

#### Election hacking doesn’t pass the severity threshold for self-defense.

Ido Kilovaty 16. Cyber Fellow at the Center for Global Legal Challenges at Yale Law School. "Towards a Cyber-Security Treaty". Just Security. 8-3-2016. https://www.justsecurity.org/32268/cyber-security-treaty/

This is because the laws of war are inapplicable to most cyber operations. The DNC Hack, for example, did not cause any physical destruction or bodily harm. It therefore does not reach the severity threshold that justifies the resort to self-defense measures (ad bellum) or the law of armed conflict (in bello). What remains, as a matter of international law, is the general norm of non-intervention, which does not say much about hostile state-sponsored activities in cyberspace.

#### Election hacking is not an armed conflict.

Ellen Nakashima 17. Washington Post. "Russia’s apparent meddling in U.S. election is not an act of war, cyber expert says". Washington Post. 2-7-2017. https://www.washingtonpost.com/news/checkpoint/wp/2017/02/07/russias-apparent-meddling-in-u-s-election-is-not-an-act-of-war-cyber-expert-says/

Russia’s hacks of the Democratic National Committee and its election meddling were alarming, but not an act of war, said a leading scholar of international law in cyber operations.

“I’m no friend of the Russians,” said Michael Schmitt, chairman of the U.S. Naval War College’s International Law Department and director of a project that analyzes how international law applies to cyber operations — especially in peacetime.

But Moscow’s hacking and dumping of Democratic emails to WikiLeaks “is not an initiation of armed conflict. It’s not a violation of the U.N. Charter’s prohibition on the use of force. It’s not a situation that would allow the U.S. to respond in self-defense militarily.”

Schmitt spoke in an interview with The Washington Post coinciding with the release of the Tallinn Manual 2.0, an updated reference for lawyers around the world on how international law applies to cyberspace. Schmitt, who is also a law professor at the University of Exeter in Britain, led the legal team that compiled the manual.

Sen. John McCain (R-Ariz.), the chairman of the Armed Services Committee, has said he believes Russia’s interference in the 2016 presidential election amounted to an act of war.

Nonetheless, Schmitt said, Russia’s apparent attempt to influence the outcome of the election by its release of emails through WikiLeaks probably violates the international law barring intervention in a state’s internal affairs. And that would give the United States grounds to undertake “countermeasures” that would otherwise be unlawful, he said.

The updated Tallinn Manual explores cyber actions most commonly confronted by states today: espionage, denial of service disruptions and influence operations — actions that fall short of armed conflict and the use of force.

“The Russians are masters at playing the gray areas” of law, said Schmitt, arguing that the Kremlin is adept at carrying out operations that fall short of breaching undisputed legal red lines that would invite robust responses. For instance, Moscow has not conducted operations in the United States that cause deaths or significant, nationwide economic harm that would warrant the use of force in response.

Hacking the DNC’s emails is an act of political espionage, which is not a breach of international law, Schmitt said.

### Link---Non-Physical Damage---2NC

#### Russian attacks won’t cause physical damage---the plan’s fiated retaliation below threshold violates IHL.

Michael Schmitt 2/24/22. Professor of International Law at the University of Reading in the United Kingdom; G. Norman Lieber Distinguished Scholar at the U.S. Military Academy at West Point; Strauss Center Distinguished Scholar and Visiting Professor of Law at the University of Texas; professor emeritus at the U.S. Naval War College; and Director of Legal Affairs for Cyber Law International. He serves on the Department of State’s Advisory Committee on International Law, is a member of the Council on Foreign Relations and a Fellow of the Royal Society of Arts, and is General Editor of The Lieber Studies (OUP). "Expert Backgrounder: NATO Response Options to Potential Russia Cyber Attacks". Just Security. 2-24-2022. https://www.justsecurity.org/80347/expert-backgrounder-nato-response-options-to-potential-russia-cyber-attacks/

Aside 2: The Application of International Humanitarian Law

Irrespective of whether prospective Russian cyber operations might constitute an internationally wrongful act, the question remains whether they might initiate, in lay terms, “war” between Russia and the targeted State. In international law, we call that an “international armed conflict” – and it brings into operation international humanitarian law (eg the Geneva Conventions) to regulate the belligerents’ conduct, including the operation itself. An international armed conflict occurs when there are hostilities between two or more States. The nature and severity of the requisite hostilities are contentious, especially with respect to cyber operations that may not be destructive or deadly. (Tallinn Manual 2.0, rule 82).

It is unfortunate that the lay term for such situations is “war.” It is crucial that diplomats, commentators and others keep distinct the legal understanding that an “international armed conflict” may exist between two States because of the introduction of force, but that force may not rise to the level of an “armed attack” triggering the right to exercise self-defense.

Causation of significant physical damage or death in the target State would likely qualify as an international armed conflict. However, States have been reticent about treating even cyber operations causing physical damage or necessitating replacement of cyber infrastructure, such as those launched by Iran into Saudi Arabia against Saudi Aramco, as such. In any event, it is unlikely that potential Russian cyber operations would be at a level triggering an international armed conflict between Russia and the target State. The more likely scenario for triggering an international armed conflict is a kinetic engagement between Russian and NATO military forces deployed forward, for instance, in the Baltic States. At that point, an international armed conflict would exist, and international humanitarian law would govern cyber operations with a nexus to that conflict.

#### ICJ rulings prove---attacks must cause physical damage to be acceptable under international law.

Michael Schmitt 2/24/22. Professor of International Law at the University of Reading in the United Kingdom; G. Norman Lieber Distinguished Scholar at the U.S. Military Academy at West Point; Strauss Center Distinguished Scholar and Visiting Professor of Law at the University of Texas; professor emeritus at the U.S. Naval War College; and Director of Legal Affairs for Cyber Law International. He serves on the Department of State’s Advisory Committee on International Law, is a member of the Council on Foreign Relations and a Fellow of the Royal Society of Arts, and is General Editor of The Lieber Studies (OUP). "Expert Backgrounder: NATO Response Options to Potential Russia Cyber Attacks". Just Security. 2-24-2022. https://www.justsecurity.org/80347/expert-backgrounder-nato-response-options-to-potential-russia-cyber-attacks/

Acting in self-defense is the least likely response. That is because a Russian cyber operation crossing the required threshold of an “armed attack” is the least likely to occur. Article 51 of the United Nations Charter provides, “Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.” Customary international law is generally in accord. Under the law of State responsibility, the right of self-defense is a “circumstance precluding wrongfulness,” that is, a situation in which a State may engage in otherwise unlawful conduct to defend itself (Articles on State Responsibility, art. 21). Most importantly, the right of self-defense allows States facing an armed attack to use force in their defense. That force may be cyber or kinetic, and the response need not be in kind; kinetic force may be used to respond to a cyber armed attack and vice versa (Tallinn Manual 2.0, rule 71).

Of course, States may defend themselves against a cyber “armed attack.” But in the current context, the right of collective defense looms even larger. That is because some of the NATO States that Russian cyber operations might target cannot mount an effective defense on their own.

In this regard, Senator Mark Warner, the Senate Intelligence Committee Chairman, has suggested the prospective Russian cyber operations could trigger Article 5 of the North Atlantic Treaty. In relevant part, the article provides:

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

NATO has repeatedly confirmed that the right of self-defense applies in cyberspace. Accordingly, the question is whether the possible Russian cyber operations might rise to the level of an “armed attack” under UN Charter Article 51 and, therefore, Article 5 of the North Atlantic Treaty.

The prevailing view is that, in the words of the International Court of Justice in Nicaragua, an armed attack is the “most grave form” of a use of force. Thus, the scale and effects of any Russian cyber operations would have to be especially severe before triggering the right of individual or collective self-defense. Physical damage or death might need to occur before consensus on classification as an armed attack could be achieved. That said, at least one NATO member, France, has taken a broad view suggesting a cyber operation would be an armed attack “if it caused substantial loss of life or considerable physical or economic damage.”

#### The emerging consensus is damage and effects based---the plan breaks it.

James A Lewis 11. Senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS), where he writes on technology, security and the international economy. Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service Officer and as a member of the Senior Executive Service. "Cyberwar Thresholds and Effects."IEEE Security & Privacy, vol. 9, no. 5, pp. 23-29, Sept.-Oct. 2011. https://ieeexplore-ieee-org.proxy.library.emory.edu/document/5719593

The emerging consensus is that a cyberspace attack produces the equivalent effect of an armed attack using physical means. If an incident doesn't produce damage, destruction, or casualties, it's not an attack. A gray area exists when deciding when the disruption of services and data rises to the level of damage or destruction equivalent to the use of force, but the simplest approach is to reason by analogy and ask whether the cyberincident creates damage equal to a kinetic attack. An effects-based definition sets a clear threshold.

### AT: No Link---Burkadze---2NC

#### Their evidence doesn’t say all cyber responses are legal.

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

---2AC CARDS ENDS---

However, every unfriendly act does not cross the use of force threshold. The International Court of Justice held that financing guerrillas, albeit an unlawful "intervention," did not fall into the same category. Therefore, cyber operations intended to economically coerce another state to engage in, or desist from, a particular course of action would not amount to a use of force; nor would financing a rebel group's cyber operations. Beyond these directly parallel examples, uncertainty remains as to where the threshold lies.2 1

### AT: No Link---Hacking = Sovereignty---2NC

#### Election hacking doesn’t violate sovereignty---expert consensus.

Alex Xiao 20. J.D. Candidate at Duke University School of Law, Class of 2020. “Responding to Election Meddling in The Cyberspace: An International Law Case Study on The Russian Interference in The 2016 Presidential Election”. Duke Journal of Comparative & International Law. Vol. 30:349. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1565&context=djcil

Violating another State’s sovereignty is a breach of an international obligation, which allows the victim State to respond with countermeasures.128 It may seem intuitive to accuse the Russian government of violating the sovereignty of the United States by engaging in cyber operations that intended to undermine a major national election. However, a close examination of international law does not support this argument.

Customary international law defines sovereignty as something that signifies “[i]ndependence in regard to a portion of the globe as the right to exercise therein, to the exclusion of any other State, the functions of a State,”129 indicating two major aspects of sovereignty: territorial integrity and State functions.130 A violation of either aspect amounts to a violation of State sovereignty.

First, with regard to territorial integrity, Tallinn Manual 2.0 experts agreed that a remotely conducted cyber operation causing either physical damage to objects (both private and governmental) or injury to persons violates sovereignty.131 In the cyber context, damage to objects not only means physical damage, but also a loss of functionality, as dysfunction of cyberinfrastructure is often the result of hostile cyber operations.132 However, Tallinn Manual 2.0 experts disagreed on the extent of the loss of functionality required to qualify as a violation of territorial integrity.133 Some insisted that there must be an irreversible loss of function, while, for others, altering or deleting data stored in the cyberinfrastructure would suffice, even if the loss of functionality might be temporary and restorable.134 An example of the former position would be the Stuxnet operation, which destroyed thousands of Iranian centrifuges,135 while a major denial-of-service attack would suffice the latter position.136 However, with respect to the Russian election meddling, neither of the positions above are likely to establish a violation of sovereignty because no known damage or loss of functionality was caused to information and communication technology in the United States.

Second, a remote cyber operation amounting to an interference of inherently governmental functions also violates the sovereignty of the victim State.137 Holding national elections would be a classic example of an inherently governmental function, which States enjoy the exclusive right to perform.138

However, as a matter of international law, it is unclear exactly what cyber activities amount to an illegal “interference” of such function. The extreme cases are clear. On the one hand, a cyber operation that affects public voting infrastructures, such as voting machines or voting registration systems, would be a clear interference of inherently governmental functions.139 On the other hand, Tallinn Manual 2.0 experts agreed that political propaganda during foreign elections would not amount to an illegal interference because prevalent opinio juris does not treat hostile political propaganda as a violation of sovereignty.140

### AT: No Link---Hacking = Illegal Intervention---2NC

#### Cyber operations are persuasion under international law---its noncoercive.

Alex Xiao 20. J.D. Candidate at Duke University School of Law, Class of 2020. “Responding to Election Meddling in The Cyberspace: An International Law Case Study on The Russian Interference in The 2016 Presidential Election”. Duke Journal of Comparative & International Law. Vol. 30:349. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1565&context=djcil

4. Breach of Legal Obligations: Illegal Intervention

The intervention in another State’s internal affairs is the second internationally wrongful act that the United States might be able to allege against Russia in order to use countermeasures. Illegal intervention consists of two elements under customary international law: (1) the operation must have an effect on the internal affairs that are part of the victim State’s domaine reserve and (2) the effect of the operation must be coercive.144 Similar to the violation of sovereignty, an operation of illegal intervention can target both private and governmental entities145 and can only be committed by a State actor.146

As the ICJ explained in the Nicaragua judgment, domaine reserve refers to “matters in which each State is permitted by the principle of sovereignty, to decide freely. . . . [F]or example, the choice of a political . . . system.”147 Employing coercive measures regarding such choices amounts to a wrongful intervention as a matter of international law.148 For the purposes of this Article, a national election clearly falls into the category of domaine reserve. The determinative question is whether the Russian election meddling operation was coercive.

Tallinn Manual 2.0 experts agreed that coercion “refers to an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way.”149 Also, “coercion must be distinguished from persuasion, criticism, public diplomacy, [and] propaganda”150 because, different from coercion, “such activities merely involve either influencing (as distinct from factually compelling) the voluntary actions of the target State or seek no action on the part of the target State at all.”151 The exact standard of coercion, however, is still underdeveloped. Just like the violation of sovereignty, the extreme cases on both ends of the spectrum are clear: in the election context, an attack disabling the voting infrastructure to prevent voters from casting their ballots would be an example of coercion, while mere espionage or propaganda campaigns would not amount to prohibited intervention as a matter of international law. 152

Therefore, the hacking of the DNC servers, disseminating the information collected from the hacking, and the propaganda campaign on both social media and the Russian State media would not constitute coercive acts. None of these activities compelled the voters to engage in involuntary actions or inactions, but, rather, they were simply influencing and persuading the voters to act in a certain way.

### AT: No Link---UN Security Council Authorizes---2NC

#### The UN won’t authorize attacks---its an independent link.

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

Article 41 permits the use of measures that do not reach the use of force threshold, including “complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations” (United Nations "Charter of the United Nations"). If Article 41 measures are not sufficient or are inadequate, the Security Council may authorize use of force measures by “air, sea, or land forces as may be necessary to maintain or restore international peace and security” (United Nations "Charter of the United Nations").

The likelihood of the Security Council making this determination and authorizing such measures is miniscule for two reasons. First, in the previous decade, the UN Security Council has not considered cyber operations of any type to be a threat to the peace, a breach of peace, or an act of aggression. Secretary General Ban Ki-Moon implored the Security Council at its 6277th meeting in 2010 to consider cybercrimes an emerging threat to international peace. The Security Coucil made no response to the request and cyber operations have not been mentioned in Council meetings related to Article 39 since that date (United Nations "Repertoire of the Practice of the Security Council"). Secondly, three of the most pervasive state cyber actors are permanent members of the Security Council with veto power. China, Russia, and the United States are unlikely to put forth any resolutions that limits their ability to maneuver in cyberspace. As they use cyber operations that become closer and closer to the threshold of the use of force or an armed attack, they will be less likely to specifically name state cyber operations a threat to the peace or an act of aggression.

### IL---Intel Norms---2NC

#### The plan militarizes intelligence norms---makes escalation more likely.

Jeppe T. Jacobsen 21. Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark "Cyber offense in NATO: challenges and opportunities". OUP Academic. 5-10-2021. https://academic.oup.com/ia/article-abstract/97/3/703/6205395

The question then arises: does the lack of capacity to deter non-military hybrid cyber activities suggest that it is time for NATO to renegotiate the scope and substance of its collective defence clause?65 When it comes to cyberspace, the next section expresses scepticism about expanding NATO’s role. It addresses the escalation risk associated with having NATO, an organization that has refocused its attention on a more traditional military threat, become a more active player below the threshold of collective defence. It argues that a more active stance outside military confrontation risks undermining the intelligence norm that currently dominates in cyberspace—a norm whereby state activity in foreign networks is not considered escalatory.

Escalation and the dominant intelligence norm

The large overlap between intelligence collection and attack in cyberspace makes it difficult to send clear signals to adversaries, in terms of either capabilities or intentions. When a foreign entity is moving around in a network, is it then about to start a military operation? Is the activity part of a reconnaissance mission? Is it political or economic espionage? Is it active defence? The difficulty of answering these questions has created much nervousness among cyber-conflict experts. Ben Buchanan, for example, has shown how defensive hacking or intelligence-gathering in cyberspace is easily misinterpreted as aggressive behaviour.66 Why, then, have we not experienced serious misinterpretation and escalation in cyberspace?

One way to explain this is through the existence and dominance of a largely unspoken but widely accepted norm. For decades, the predominant actors in cyberspace have been intelligence agencies; and the norms that characterize interactions between intelligence agencies are not primarily concerned with military concepts such as conflict escalation and deterrence.67 In the world of intelligence agencies, success is not about keeping a distance between oneself and the adversary by signalling one’s intentions and capabilities. It is about being able to outmanoeuvre adversaries in a space of constant contact.68 There are always risks, and the work usually takes place in legal grey zones where a clear distinction between war and peace is not the guiding principle. This is an arena where the opportunity to annoy, cheat and delay opponents is taken when it arises. In short, espionage and counter-espionage do not fit well with the thorough military operational planning that characterizes NATO operations. Intelligence operations, on the other hand, fit perfectly with a dynamic cyberspace where anonymity is easy to achieve and uncertainty a constant condition.69 The states that embrace cyberspace as a domain where the intelligence norm dominates are able to use a broader array of tools to pursue or respond to various foreign political objectives than only those that relate to military operations.

In its 2018 ‘vision’, the US Cyber Command built implicitly on the dominant intelligence norm. Here, the objective is to become more agile and act as close to the adversary as possible (‘defend forward’).70 The United States considers ‘constant contact’ and ‘persistent engagement’ as the necessary guiding principles to achieve superiority in cyberspace and to take full advantage of the broader potential for pursuing its political objectives through cyberspace. During the 2018 US midterm elections, for example, the US Cyber Command worked closely with the NSA to disrupt servers operated by the Russian Internet Research Agency aiming to spread fake news and stir up tension in the United States.71 More recently, the US Cyber Command responded with various cyber effects against Iran after the Iranian Revolutionary Guards apparently placed mines on ships in the Strait of Hormuz.72 These practices illustrate that, for the United States, cyber effects provide political options when one does not want to escalate existing tensions into military confrontation. Defensive coordination between allies through CYOC supports such defensive use of cyber effects, increasing the possibility that US Cyber Command will be allowed to ‘defend forward’ and work persistently through allied networks.73 A more cyber-active NATO, however, risks being counterproductive to the ambition to ‘defend forward’ through allied networks.

Unintended conflict escalation from ongoing cyber activity is mainly a risk if military analysts—in a strategic environment with heightened attention to military confrontation—ignore the dominant intelligence norm. If that happens, it becomes more likely that ‘persistent engagement’ and active cyber defence will be misinterpreted as military preparation, armament or the initial phase of an attack. If NATO, an organization that has publicly returned to its original raison d’être of deterrence and collective defence, becomes the entity that coordinates cyber effects below the threshold of armed conflict, then the likelihood increases that Russia misinterprets these effects as escalatory and acts accordingly. In other words, a more active NATO in the current strategic environment increases the risk that the existing intelligence norm will be undermined and replaced by a more militarized norm.

### IL---Modeling---2NC

#### The plan models a lower threshold for use of force---others look to the US.

Robert D. Sloane 08. Associate Professor of Law, Boston University School of Law. “The Scope of Executive Power in the Twenty-First Century: an Introduction” Boston University Law Review 341 (2008). https://moam.info/boston-university-school-of-law\_59d0337c1723dd68706a8f07.html

Because of the nature of the international legal and political system, what U.S. Presidents do and say often establish precedents that strongly influence what other states do and say – with potentially dramatic consequences for the shape of customary international law. The paradigmatic example is the establishment of customary international law on the continental shelf following the Truman Proclamation of September 28, 1945,55 which produced an echo of similar claims and counterclaims, culminating in a whole new corpus of the international law of the sea for what had previously been understood only as a geological term of art.56

Many states took note, for example, when in the 2002 National Security Strategy of the United States (“NSS”), President Bush asserted that the United States had the right under international law to engage in preventive wars of self-defense.57 While, contrary to popular belief, the United States never in fact formally relied on that doctrine in practice, many would argue that President Bush de facto exercised this purported right when he initiated an armed conflict with Iraq based on claims, which have since proved unfounded, about its incipient programs to develop catastrophic weapons. The 2006 NSS notably retreats from the 2002 NSS’s robust claims of a right to engage in preventive wars of self-defense.58 Yet even within this brief, four-year period, an astonishing number of other states have asserted a comparable right to engage in preventive self-defense. These include not only states that the United States has described as “rogue states,” such as North Korea and Iran, but Australia, Japan, the United Kingdom, China, India, Iran, Israel, Russia, and (though technically not a state) Taiwan.59 I doubt we will welcome the consequences of this pattern for the evolving jus ad bellum of the twenty-first century.

### Impact---International Law/AT: Realpolitik---2NC

#### International law contains violence---assumes realpolitiks.

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 fact that international law is often dismissed as window-dressing on Realpolitik is misleading. Such an approach understates the importance of international agreements in maintaining peace and security. For liberal democracies that respect the rule of law, international law undoubtedly shapes and bounds governments' activities. At a time when the action's of unscrupulous states and violent extremist groups continue to threaten peace and security internationally, it is even more important that such actions are countered with a strong commitment to existing international law and the values that it represents.'

#### International law solves incentives for conflict---realism ignores background norms.

Annabelle Timsit interviewing Oona Hathaway, and Scott Shapiro 17. Hathaway and Shapiro are Yale law professors. "When the World Outlawed War". Atlantic. 10-19-2017. https://www.theatlantic.com/international/archive/2017/10/the-internationalists-war-peace-oona-hathaway-scott-shapiro/542550/

Timsit: Your book’s thesis that law alone has stopped war is controversial. What would you respond to realist critics of your book, who say it’s really just power that matters?

Hathaway: Realists fail to understand how law works. … When it is most effective, the law does not induce states to act contrary to incentives; it changes those incentives themselves. To take one example: After war was outlawed, conquest was no longer legal. As a result, when Japan invaded Manchuria in 1931, the U.S. and the states that were party to the League of Nations refused to recognize the conquest, pointing specifically to Japan’s violation of its legal obligations under the Pact, which Japan had ratified. This change in the rules thus changed the incentives states faced—they could still seize land with force, but they could no longer enjoy the fruits of their conquests.

The realist might respond that, even if the change in the law changes behavior, that doesn’t prove that law matters: The law is simply a tool of the powerful—great nations create law that is in their interests, and when the law changes behavior, power is doing the causal work, not the law. But to say that the powerful shape the law to reflect their interests is not to say that law is merely a byproduct of power. Power may lead to rules, but rules take on lives of their own. They change behavior by changing the incentives for action—not just for the weak but for the strong as well.

Scott Shapiro: So much of our book is an attempt to show that the law is playing such a strong role in the way states behave that we don’t even notice it. It’s hiding in plain sight. So it’s kind of a triumph of the outlawry of war that we don’t even recognize it at work. But, even though we’re lawyers and think law is really useful, we also think that the law has limits, that is, that there’s not always a legal answer to all the questions that arise. When that happens, there are arbitral bodies [such as] the International Court of Justice.

### AT: UN Failing---2NC

#### The impact is linear---current UN is better than complete dissolution.

Dr Shashi Tharoor 2/27/22. Third-term MP for Thiruvananthapuram. "Russia-Ukraine War: Even a Weak United Nations is Better Than No United Nations". TheQuint. 2-27-2022. https://www.thequint.com/voices/opinion/russia-ukraine-war-even-a-weak-united-nations-is-better-than-no-united-nations-vladimir-putin-zelenskyy

UN is Both a Stage and an Actor

The UN works best when its member states on the Security Council can agree on an issue, and deploy the human, material and military resources needed to address it. When the political will for agreement is absent, and worse, when the superpowers are divided, the UN cannot act.

It is still a useful forum for states to vent their opinions and frustrations on issues, as the debate on Ukraine demonstrated. The US went ahead with its Security Council resolution knowing full well that it would be vetoed, knowing that the debate would reveal the principles and stake and show up Russia’s relative isolation in the world.

Indeed, though three states, including India, abstained, no one voted alongside Russia against the resolution. The “demonstration effect” served a purpose too.

Let’s not forget the UN is both a stage and an actor. It is a stage for its member states to declaim their differences and celebrate their convergences; and it is an actor, in the shape of its Secretary-General, its various agencies and its peace-keeping forces, to execute what those member states agree upon.

UN's Limitations Need to be Understood with an Open Mind

Some Secretaries-General are able to rise above the status of “international civil servant” to command a moral presence on the world stage. Dag Hammarskjold and Kofi Annan, both Nobel laureates, are examples.

Annan was even described as a “secular Pope”. When they spoke, the world listened.

The current Secretary-General, Antonio Guterres, a well-meaning former Portuguese Prime Minister, resorted to the pulpit himself when he appealed to Russia “in the name of humanity” to stop its invasion. But the limits of moral suasion were apparent in the way his appeal went unheeded, and without response.

At the height of the Cold War during the 1950s, Hammarskjold was asked about the limitations of the organisation, and replied pithily: “the United Nations was not created to take mankind to heaven, but rather, to save humanity from hell.”

His point was clear: one should not seek perfection from an institution of member states which would always be, more or less, the sum of its parts. But an imperfect United Nations was better than none at all.

Let's Be Grateful for the UN We Have

The long-serving Soviet Ambassador to the UN in the 1960s, Yakov Malik, famously said that people dismissing the UN as an ineffective body reminded him of an old story about Adam and Eve in the Garden of Eden. Adam, he said, found that Eve was being indifferent to him; so he asked her, “Eve, is there someone else?”

That’s the point about the UN – is there anything else? It may be helpless and hopeless sometimes, but it is the only global platform where every government in the world can come together to discuss issues and policies, raise global consciousness and when possible, agree on meaningful action.

If the United Nations did not exist, today’s divided world would be incapable of inventing it. Let’s be grateful for the UN we have. We’d be much worse off without it.

### AT: Norm Violation---2NC

#### Norms delay and prevent violation.

Henry Farrell and Charles L. Glaser 17. George Washington University. "role of effects, saliencies and norms in US Cyberwar doctrine". OUP Academic. 3-31-2017. https://academic.oup.com/cybersecurity/article/3/1/7/3074707#64534665

Another possible criticism is that states often violate norms and specifically that they have often violated the norms against harming non-combatants. Hence, one might argue that norms are effectively worthless. However, in wars of attrition, states have often not violated the norm against targeting civilians until late in the war, and violate the norm out of determination or even desperation to win [40]. If the same logic applied to cyber war, then a norm against counter-infrastructure attacks could contribute to delaying these attacks and possibly thereby avoiding them.

### AT: LOAC Bad---Counterforce---2NC

#### No link to LOAC turns---the plan doesn’t eliminate LOAC but extends the definition of “armed conflict” in UN Article 51.

#### Eliminating LOAC is insufficient to solve---structural factors make counterforce inevitable.

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

We recognize that a variety of other factors lend support to the US preference for counterforce, including military organizational interests in modernized and technically advanced forces,25 the demands of maintaining morale within the nuclear commands,26 and worse-case planning that understandably influences nuclear strategy when the adversary’s decision criteria and decision calculus cannot be entirely known. These factors are sufficient on their own to explain the US commitment to counterforce and its pursuit of damage limitation. Nevertheless, adding (or continuing to develop and sharpen) another sophisticated, appealing, and easily understood set of guidelines that favors counterforce risks widening the internal coalition of government players who favor counterforce and provides current proponents with a powerful argument. Our hope is that the United States will eventually reject its counterforce doctrine against major powers. Taking the LOAC off the table will not be sufficient to bring about this radical change. But accepting the LOAC guidance for US nuclear strategy will make accomplishing this transformation still more difficult.