## AT: Mutual Restraint Counterplan

### Perm---2AC

#### Perm do both---deterrence helps cyber arms control treaties.

Mette Eilstrup-Sangiovanni 17. Department of Politics and International Studies, University of Cambridge, Cambridge, UK. "Why the World Needs an International Cyberwar Convention". SpringerLink. 7-21-2017. https://link.springer.com/article/10.1007/s13347-017-0271-5

Let me be clear at the outset about what I am not arguing: I do not advocate that political and military leaders abandon current objectives of bolstering cyber deterrence in favor of a singular reliance on international diplomacy to manage cyber rivalry. Just like during the Cold War’s nuclear standoff, international arms control and strategic deterrence must go hand-in-hand if we are to succeed in reducing the risk of global cyber conflict. However, I argue, creating an international legal framework to govern cyber warfare would abet efforts to achieve stable cyber deterrence. Indeed, many of the problems that currently undermine effective cyber deterrence (including difficulties of attribution, difficulties in distinguishing hostile attacks from innocent mistakes, lack of clarity about what constitutes an attack under international law, and—closely related to this—lacking credibility of retaliatory threats) would be greatly alleviated by the articulation of clear, binding international rules and norms that would both serve to distinguish lawful from unlawful behavior and facilitate punishment of cyber aggressors. My argument, in other words, is that international arms control and the desire to strengthen states’ individual capacities to deter cyber aggressors are not antithetical goals but present mutually supportive strategies.

### Delay---Negotiations---2AC

#### Delay---negotiations take too long

Martha Finnemore 11. Professor at the Elliott School of International Affairs at George Washington University “Chapter VI: Cultivating International Cyber Norms”. https://citizenlab.ca/cybernorms2011/cultivating.pdf

One common reaction to coordination problems, particularly in the international sphere, is to negotiate a treaty and make binding or “hard” law on the topic. There are obvious advantages to this. Treaties have the force of law. Theoretically, there should be enforcement by governments of their provisions. Treaties also offer at least an illusion of clarity since they usually spell out details of the agreement and explain rules in great detail. But negotiating treaties can be a slow and cumbersome process, ill-suited to fast-changing issues like cyber security and Internet governance. Governments may also not be the best or only actors to be making rules in this area since so much of the technology is in private hands.

### Enforcement---2AC

#### Not enforceable.

Scott Neuman and Greg Myre 21. Scott Neuman Writer/Editor, Digital News @ NPR. Greg Myre National Security Correspondent @ NPR. "Hacks Are Prompting Calls For A Cyber Agreement, But Reaching One Would Be Tough". NPR.org. 7-2-2021. https://www.npr.org/2021/07/02/1009925791/hacks-are-prompting-calls-for-a-cyber-agreement-but-reaching-one-would-be-tough

Such discussions have been kicking around for years, but many cyber experts remain deeply skeptical that such an agreement could be reached, let alone enforced.

Cyber strikes are low-cost and high-reward

The first big challenge would be simply getting everyone to agree to the rules. Russia, China, Iran and North Korea have all been blamed for significant hacks against the U.S., and analysts say those countries see cyber strikes as cheap, effective and easy to deny.

It's not even clear if such countries would be willing to actually agree to terms, because cyber attacks for them are "really useful in their geopolitical positioning," April Falcon Doss, a former National Security Agency official who now heads a technology program at Georgetown's law school, tells NPR.

Compared to the arms agreements between the U.S. and Soviet Union, a cyber treaty would be extremely difficult to monitor and enforce. That's because the production, development and stockpiling of nuclear, biological and chemical weapons is fundamentally different from the ephemeral nature of cyber weapons, says Doss.

"If the question is whether or not a signatory to a nuclear arms control treaty is building up their nuclear stockpile, there will almost certainly be some evidence, factory production, storage of nuclear weapons," she says. "There will be satellite imagery or there will be on the ground reports."

Tests of nuclear weapons or ballistic missiles, such as those carried out by North Korea in recent years, are also relatively simple to monitor compared to the challenge of keeping an eye on the dark corners of the Internet to track down new cyber weapons, Doss says.

"Detecting their development is much harder because you don't have big stockpiles of missiles sitting around and there's nothing that's visible in that sense," she says.

Thomas Graham, a U.S.-Russia expert at the Council on Foreign Relations, says any analogy to a Cold War-style arms agreement would be tenuous.

"We're dealing with computer code. So this is radically different from some nuclear weapons," he tells NPR.

### Say No---2AC

#### Say no---fundamental differences.

Robert G. Papp 19. Retired in 2017 after service as a naval officer and a career in federal civil service, including as director of the Center for Cyber Intelligence at the Central Intelligence Agency. PhD from Columbia University. “A Cyber Treaty with Russia”. https://www.wilsoncenter.org/sites/default/files/media/documents/publication/kennan\_cable\_no.\_41.pdf

Prospects for meaningful cyber negotiations with the Russian Federation, let alone a bilateral agreement or cyber treaty, seem almost impossible to imagine today. Our anguish over Russia’s meddling in American elections, preoccupation with alleged ties between the Trump administration and the Russian government during the recently concluded Mueller investigation, and major disagreements on geopolitical issues including Ukraine, Syria, and Venezuela, have left us at an impasse. Instead of genuine dialogue between the United States and Russia, we see the two nations talking past each other and posturing to both domestic and international audiences.

More alarmingly, the very framework of bilateral and multilateral arms control treaties that got us through the last decades of the Cold War, starting in 1972 with the Anti-Ballistic Missile (ABM) Treaty and the interim Strategic Arms Limitation Agreement (SALT I), is in disarray. This process of unraveling likely began in 2002 when the U.S. withdrew from the ABM Treaty. The Russian Federation suspended its participation in the1992 Conventional Armed Forces in Europe Treaty in 2007 and completely halted its participation in 2015. Most recently, the U.S. announced, on February 22, 2019, its intent to withdraw from the Intermediate-Range Nuclear Forces (INF) Treaty signed in 1987.

Given these developments, proponents of treaties with Russia, whether bilateral or multilateral, now seem few and far between. Even the architects of past agreements must justifiably wonder what has become of their life’s work. How, then, might negotiations leading to a cyber treaty be a viable policy option?

### XT---Say No---1AR

#### Say no---different expectations

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

The cyber operations detailed in Chapter 2 vary greatly in scale and scope. The victim states responded to the operations with varying types and levels of countermeasures. Because nation-state use of cyber operations is increasing in frequency year on year, the need for an international law framework is growing. Chapter 3 explores the application of existing international law to cyber operations with the specific focus on pre-war conditions. This research does not focus on cyber operations as they relate to the law of armed conflict. A nation’s understanding of this application applies directly to its use of cyber operations and can shed significant light on an adversary’s possible actions. Agreement between Moscow and the West on the threshold of cyber-attacks below the level of armed conflict may be difficult. Russia and the West have quite different views on what is a retaliation-worthy attack (Segal The Hacked World Order : How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age 105). In 1996, the US and Russia secretly met in Moscow to discuss a possible international treaty framework, specifically relating to cyberspace, but no agreement was reached.

### XT---Say No---AT: Eilstrup-Sangiovanni---1AR

#### Concedes negotiations are fraught!

NOTE---ICWC = International Cyberwar Convention

Mette Eilstrup-Sangiovanni 17. Department of Politics and International Studies, University of Cambridge, Cambridge, UK. "Why the World Needs an International Cyberwar Convention". SpringerLink. 7-21-2017. https://link.springer.com/article/10.1007/s13347-017-0271-5

The arguments presented in this article should not be read as a statement of ingenuous optimism. Negotiating an ICWC will be fraught with difficulty given the diverse interests at stake, and the task will not be accomplished overnight. Nonetheless, I argue, most standard objections to embarking on a process of international negotiation (including difficulties of verifying compliance and problems of rapid technological change) fail on closer inspection. In the end, the main barrier to an international agreement on governing cyberconflict may be opposition by powerful (mainly) western states, whose desire to exploit current strategic advantages in the cyber-domain leads them to reject a treaty. For example, many observers judge that America’s enduring hostility towards binding international rules for cyberspace is driven largely by its technological superiority in the realm of tactical electronic warfare, which provides a strong incentive to maintain maximum freedom of action in this domain (see Baruah 2013; Clarke and Knake 2010; Sanger 2015; Lindsay 2015, 46, 61–62; Sanger 2015; Goldsmith 2011). Not only would America be reluctant to bargain away its ability to exploit current tactical advantages, but as the world’s strongest cyber power, American decision-makers may fear that by accepting binding international constraints on the conduct of cyber warfare, they would be trying their own hands while allowing other nations to rapidly catch up (see Singer and Friedman 2014).

### Internet Freedom DA---2AC

#### Russia uses the counterplan to shut down internet freedom.

Todd Prince 19. Senior correspondent for RFE/RL based in Washington, D.C. "U.S. Concerned Russia-Backed UN Resolution Will Hurt Online Freedom". RadioFreeEurope/RadioLiberty. 12-20-2019. https://www.rferl.org/a/us-russia-internet-un/30335318.html

The resolution -- Countering The Use Of Information And Communications Technologies For Criminal Purposes -- would create a new cybercrime treaty written by Russia, a country analysts have said is cracking down on Internet freedom at home to stifle opposition to the Kremlin.

“The Russians clearly are interested in pushing their vision of what the Internet should look like in the future, and that’s conflating this idea of cybercrime with cybersecurity and cyber controls,” a State Department official told media on December 19.

Russia wants “a form of lockdown on information” over the Internet and a “curtailment of those freedoms” that the United States stands for, the State Department official said.

The UN General Assembly vote comes less than two months after Russia’s so-called “sovereign Internet” law came into force. The controversial law requires providers to install equipment that could route Russian web traffic through points that are controlled by the state. Critics say “sovereign Internet law” legislation is an attempt to increase censorship.

Pass The UNGA

Washington fears the UN General Assembly will pass the bill because many countries don’t understand the complexities, the official said. Russia has also been lobbying countries for years about the issue.

“On its surface, certainly a cybercrime treaty sounds like a good idea. Who wouldn’t want it? The problem is in trying to explain to those countries not as familiar with this issue set that there are mechanisms already existent and that what the Russians are really driving at is a problematic issue,” the official said.

#### That collapses human rights.

Josette Shiner 06. Former US under secretary of state for economic, business and agricultural affairs. "Why global internet freedom matters". https://www.ft.com/content/b2a89236-db8d-11da-98a8-0000779e2340

Defining and preserving internet freedom is a key and growing challenge. In an astonishingly short period of time the internet has become the greatest purveyor of news and information in history and a potent catalyst for innovation and commerce. From a small band of university researchers sharing documents to more than a billion people now connecting in real-time around the globe, the internet has proven to be a force multiplier for freedom, in even the most remote corners of the globe.

But the internet has also become a lightning rod for repressive governments as they try to restrict or block freedom of expression. Right now there are people imprisoned in countries like China, Cuba, and Iran simply for expressing their peaceful views online. The United States is determined to maximise the free flow of information over the internet and minimise success by repressive regimes in censoring information and silencing legitimate debate in this global town hall. Nonetheless, we oppose illicit online activities, such as copyright infringement, child pornography crimes, and criminal incitement to commit violent acts.

In recent months, numerous journalists have detailed the complex moral calculus that emerges when governments — such as China’s — try to control freedom of expression on the internet.

Fundamentally, internet freedom stems from the principles of freedom of expression enshrined in the Universal Declaration of Human Rights and human rights law. On this basis, we oppose the efforts of non-democratic governments to misuse the internet to restrict freedom of expression or to track and prosecute dissidents. Promoting access to information over the Internet can advance the goals of good governance, economic development, support for innovation, and a vibrant civil society. Transparency — informing users about changes or restrictions on content — holds governments engaged in censorship accountable for their actions. More broadly, effective rule of law is essential when companies are asked to turn over internet user data or to block Internet information.

#### Allowing human rights abuses is morally unacceptable and causes war

William W. Burke-White 04. Lecturer in Public and International Affairs and Senior Special Assistant to the Dean at the Woodrow Wilson School of Public and International Affairs, Princeton University and Ph.D. at Cambridge, “Human Rights and National Security: The Strategic Correlation”, The Harvard Human Rights Journal, Spring, 17 Harv. Hum. Rts. J. 249, Lexis)

This Article presents a strategic--as opposed to ideological or normative--argument that the promotion of human rights should be given a more prominent place in U.S. foreign policy. It does so by suggesting a correlation between the domestic human rights practices of states and their propensity to engage in aggressive international conduct. Among the chief threats to U.S. national security are acts of aggression by other states. Aggressive acts of war may directly endanger the United States, as did the Japanese bombing of Pearl Harbor in 1941, or they may require U.S. military action overseas, as in Kuwait fifty years later. Evidence from the post-Cold War period  [\*250]  indicates that states that systematically abuse their own citizens' human rights are also those most likely to engage in aggression. To the degree that improvements in various states' human rights records decrease the likelihood of aggressive war, a foreign policy informed by human rights can significantly enhance U.S. and **global security**.

Since 1990, a state's domestic human rights policy appears to be a telling indicator of that state's propensity to engage in international aggression. A central element of U.S. foreign policy has long been the preservation of peace and the prevention of such acts of aggression. [2](http://www.lexis.com/research/retrieve?_m=62d5bddd50e555db7dfb40b14668cef6&csvc=bl&cform=searchForm&_fmtstr=FULL&docnum=1&_startdoc=1&wchp=dGLbVzW-zSkAW&_md5=a81b07a0a90d95be59f9b7bb9d939181#n2) If the correlation discussed herein is accurate, it provides U.S. policymakers with a **powerful new tool to enhance national security through the promotion of human rights**. A strategic linkage between national security and human rights would result in a number of important policy modifications. First, it changes the prioritization of those countries U.S. policymakers have identified as presenting the greatest concern. Second, it alters some of the policy prescriptions for such states. Third, it offers states a means of signaling benign international intent through the improvement of their domestic human rights records. Fourth, it provides a way for a current government to prevent future governments from aggressive international behavior through the institutionalization of human rights protections. Fifth, it addresses the particular threat of human rights abusing states obtaining weapons of mass destruction (**WMD**). Finally, it offers a mechanism for U.S.-U.N. cooperation on human rights issues.

### XT---Internet Freedom Link---1AR

#### Russia uses the treaty to attack internet freedom---collapses human rights.

Deborah Brown 21. Senior Researcher and Advocate, Digital Rights. "Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights". Human Rights Watch. 8-13-2021. https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights

A global comprehensive treaty to counter cybercrime first proposed by Russia has gained enough support at the United Nations for negotiations to begin early next year. In addition to the irony of a government that faces criticism for turning a blind eye to cybercriminals operating within its borders pushing a global cybercrime treaty, the proposal is dangerous. A binding international treaty has the potential to expand government regulation of online content and reshape law enforcement access to data in a way that could criminalize free expression and undermine privacy.

Until now, there has been very little scrutiny of this process from a human rights – as opposed to a geopolitical – perspective. A closer look at who is proposing the treaty, the way many states have defined “crime” in the cyber context, how efforts to fight cybercrime have undermined rights, and the shortcomings of multilateral negotiating processes reveals the dangers that this treaty process poses.

In recent years, there has been a surge in cybercrime laws around the world, some of which are overly broad and undermine human rights. Governments often use them to persecute journalists, human rights defenders, technologists, opposition politicians, lawyers, religious reformers, and artists. Many governments, including some that are most supportive of a global treaty, treat forms of free expression such as criticism and dissent as crimes. A cybercrime treaty that normalizes this approach runs counter to human rights obligations.