## Mutual Restraint Counterplan

### OFF

#### The United States federal government should offer an agreement of mutual cooperation and restraint in cyberspace, with at least the Russian federation, that requires each side to restrain from information warfare and guarantees cyber non-intervention.

#### The counterplan solves the case through Russian restraint and avoids codifying retaliation to below threshold attacks. Deterrence is insufficient.

Jack Goldsmith 17. Jack Goldsmith is the Learned Hand Professor at Harvard Law School, co-founder of Lawfare, and a Senior Fellow at the Hoover Institution. "Contrarian Thoughts on Russia and the Presidential Election". Lawfare. https://www.lawfareblog.com/contrarian-thoughts-russia-and-presidential-election

“We assess Moscow will apply lessons learned from its campaign aimed at the U.S. presidential election to future influence efforts in the United States,” says the U.S. intelligence community in the most important sentence in its dismayingly evidence-free report on Russian activities in the presidential election. But how is the United States going to check these future influence efforts?

Simplifying a great deal, when a nation is vulnerable to a foreign threat it has three courses of action to improve its situation: (1) It can raise its defenses; (2) it can credibly threaten greater consequences for the attacker, thereby deterring the attacker from action; or (3) it can cut a deal in which it pledges to forego certain actions in exchange for relief from the threat by the adversary. I think the U.S. government focuses too much on (1) and (2) and not enough on (3).

The United States is not close to raising its defenses adequately and likely will not in the foreseeable future. Offense has too great an advantage over defense. We have too many soft targets and are constantly surprised when new ones are attached or exploited. (The government was stupefied by the OPM hack, and the Sony hack, and the DNC hack, among many others.) And we lack the consensus needed to take the controversial steps that would truly raise our cyber defenses.

As is evident in the Obama administration’s failure to respond to earlier Russian penetration of networks in the White House, Pentagon, and State Department, and in its relatively tepid response to the highly destabilizing DNC hack, deterrence is simply not going to work in this context. The United States has the most powerful military in the world, including the greatest capacities in offensive cyber. But it cannot use these tools to credibly commit to retaliate powerfully against harmful cyber operations, especially ones that fall below the “use of force” or “armed attack” thresholds. Attribution, especially credible attribution in public, is a very large challenge. And the United States significant digital dependencies mean that it loses in escalation in cyber because, as President Obama explained, “our economy is more digitalized and it is more vulnerable, partly because we are a wealthier nation and we are more wired than some of these other countries and we have a more opened society and we are engaged in less control or censorships of over what happens on the internet.” It’s also clear that the vaunted “name and shame” strategy simply doesn’t work in high-stakes contexts. “The idea that somehow public shaming is going to be effective, I think doesn’t read the thought process in Russia very well,” Obama noted. You don’t have to take my word that deterrence isn’t going to get the job done; as DNI James Clapper said last week: “We currently cannot put a lot of stock, at least in my mind, in cyber deterrence. … It is … very hard to create the substance and psychology of deterrence, in my view.”

That leaves (3), cutting a deal. I’m not talking about squishy cyber “norms.” There is a lot of happy talk about cyber norms, but this talk is almost always about how the United States can force adversaries to agree to the rules of the road that it likes best. I am talking about an agreement of mutual restraint: the United States agrees to restrain itself in its activities in foreign networks in exchange for restraint from our adversaries in our networks. As I wrote six years ago:

U.S. cybersecurity policymakers are in the habit of thinking too much about those who attack us and too little about our attacks on others. Creating norms to curb cyberattacks is difficult enough because the attackers’ identities are hard to ascertain. But another large hurdle is the federal government's refusal to acknowledge more fully its many offensive cyber activities, or to propose which such activities it might clamp down on in exchange for reciprocal concessions by our adversaries.

I have expressed skepticism about treaties as a solution to disorder in the cyber realm, and some of the basis for that skepticism, including attribution difficulties, applies to any form of agreement in this context. But I am increasingly of the view that the only way that the United States can get relief from damaging foreign cyberoperations is to significantly restrain its own cyberactivities abroad.

The first step to understanding here, I think, is to try to put oneself in the skin of the adversary, to understand how it sees the world and why it acts the way it does. The United States is angry because of the consequential Russian intervention in the election. But it is important to understand that the United States is widely perceived by Russia to intervene in Russian domestic affairs in ways that are just as offensive and threatening, at least to the leadership in Russia, and just as violative of Russian sovereignty.

For example: Putin attributes the embarrassing and destabilizing protests that began in Russia after the December 2011 legislative election to Secretary of State Hillary Clinton’s charges of voter fraud in the election and the “signal” her State Department sent to opposition leaders in Russia. He also claimed that the United States was responsible for the Panama Papers, which he described as and “attempt to destabilize the internal situation” in Russia. NATO’s enlargement to many former Soviet states, especially to the Baltic States in 2004, when Putin was President of Russia, was not an intervention in Russia’s domestic affairs per se, but it was an embarrassing and threatening intrusion into Russia’s sphere of influence. So too was the extension of missile defense systems to eastern Europe.

But perhaps nothing is as threatening as the pledges and activities associated with the U.S. “Internet Freedom” initiative, which (among other things) involves funding and technical support to empower citizens in authoritarian states to circumvent censorship and promote speech there. Russia views this initiative as “a U.S. strategy to intervene in [its] domestic politics through cyber means,” as David Fidler notes. To get a sense of the extent to which the Russian (and Chinese) governments are threatened by the core elements of the U.S. Internet Freedom initiative, and (relatedly) of the social media and related tools of the U.S. internet technology industries, consider four of the six “main threats in the field of international information security” listed in the 2015 Russia-PRC Cyber pact (a poor translation, but the gist comes through):

The Parties believe that the main threats to international information security are the use of information and communication technologies:

1) to carry out acts of aggression aimed at the violation of the sovereignty, security, territorial integrity of States and a threat to international peace, security and strategic stability;

2) for the application of economic and other damage, including through the provision of a destructive impact on the objects of the information infrastructure; …

5) to interfere in the internal affairs of States, violations of public order, incitement of ethnic, racial and religious hatred, propaganda of racist and xenophobic ideas and theories that give rise to hatred and discrimination, incitement to violence and instability, as well as to destabilize the internal political and socio-economic situation, violation of government;

6) for the dissemination of information harmful to the socio-political and socioeconomic systems, spiritual, moral and cultural environment of other States.

In short, China and Russia, among our most potent adversaries, see efforts to weaken their control over their networks as a direct threat to their core sovereign interests. They view it in the same way that we view the intervention in our election.

This latter point is surprising to many. A casual consumer of the news in the United States would think that the United States is the main victim in the confrontations going on in the cyber realm. It is indeed a victim. But the United States is also widely perceived around the world as the greatest threat in the cyber realm. It has, as President Obama bragged last Fall, greater offensive cyber capabilities than any other nation. And it is perceived abroad to use these capacities aggressively. Stuxnet, now widely attributed to the United States, is one example. The Snowden revelations were an even bigger deal. They provided clear, extensive, concrete evidence about the numerous impressive (and, to many, shocking) ways that the United States penetrates and collects information in foreign networks. And of course the United States isn’t taking all of the information stolen from foreign networks and putting it in a box. It uses the fruits of its espionage and theft to bolster every element of its foreign and defense policy, and its national and economic security.

It’s also worth noting, in this context, the many episodes in which the United States has intervened in foreign elections. I summarized some of the evidence in posts last summer. A study by Dov Levin found that during the Cold War, the United States intervened to influence foreign elections over twice as often (69% to 31%) as the Soviet Union. In many of these cases the United States “weaponized information” to sway the election. U.S. electoral intervention continued after the Cold War. A prominent example is its support of the populist Boris Yeltsin in the 1996 Russian presidential election. “[W]e’ve got to go all the way in helping in every other respect” besides a nominating speech, Bill Clinton told Russia advisor Strobe Talbott, who further explained in his memoir that Clinton visited Moscow in April 1996 “for no other purpose than to give Yeltsin a pre-election boost.” The Clinton administration gave Yeltsin other forms of political support, and ensured that the IMF gave Russia a $10 billion loan in what the New York Times described as a “major election-year boost for” Yeltsin. Other post-Cold War examples include the U.S. financing of “Syrian political opposition groups and related projects, including a satellite TV channel that beams anti-government programming into the country” (another example of “weaponizing information”); similar activities in the 2000 Yugoslav election, which Levin concludes was “decisive” in defeating Milosevic; and (according to David Ignatius) the aborted U.S. covert action in the Fall of 2004 to influence elections in Iraq.

In response to this history, I hear many people say some version of: “But the United States has never doxed another country covertly in the middle of a democratic election.” We don’t actually know that, but we do know this: The United States has covertly stolen information from foreign political parties, it has weaponized information, and it has influenced foreign elections. Perhaps the United States has not done these three things together, at least on the scale of the Russia operation. But the precise contours of U.S. action abroad do not define lawful or appropriate behavior, such that our adversaries feel compelled to do to us only what we do to them. The main point is that the United States is widely seen to engage in activities in other countries, including Russia, that are analogous to the DNC hack and that are viewed to threaten core sovereign interests abroad.

I should be clear, in a probably futile effort deflect charges of Russophilia (or worse), that I am not making a normative judgment here. Obviously there are huge differences in substance between (i) intervening in a foreign nation to disrupt democratic processes and (ii) intervening in a foreign nation to promote democracy and free speech. My normative preferences, for what they are worth, are for the United States to exploit its offensive advantages in cyber to collect whatever information serves our national interests, to use this information in ways that serve our interests, and to promote those interests further by spreading the U.S. conception of freedom of speech and thought to other nations.

The question is whether these are realistic goals. I think they are not, given the clear costs that the United States is suffering and will continue to suffer in the cyber realm. I don’t think the United States can continue unabated with all of its aggressive cyber actions abroad—intelligence collection, cyber attacks, information operations, and especially operations that undermine control abroad—if it wants relief from the cyber operations that are proving to be so damaging to U.S. society. Rather, I think the only hope it has to gain relief from these devastating cyber actions—or, at a minimum, a hope worth exploring—is to give our adversaries relief from our cyber actions that they perceive to be devastating. I am not talking about a treaty. But I am talking about an explicit understanding with major cyber adversaries, akin to understandings about the rules of espionage during the Cold War, that the United States will not engage in certain specific disruptive actions in exchange for desirable restraint by adversaries in U.S. networks.

Cooperation in the cyber realm will not be easy, even on a bilateral basis. There are many hurdles, some of which I outline here in the context of treaties. Attribution will always be a problem. It might not be possible to agree on the precise elements of mutual restraint. And it is possible that a spiraling tit for tat is the only compelling logic here, and that the United States will lose overall due to its digital vulnerabilities. I don’t minimize the hurdles. I only want to suggest that the option of mutual restraint should be explored.

I don’t think that U.S. intelligence collection capabilities per se are at stake. What our authoritarian adversaries really care about—where they are vulnerable in ways analogous to U.S. vulnerabilities in the recent election—are U.S. efforts to use its cyber and related capabilities in ways that are deemed disruptive to their domestic orders, i.e. the very thing the United States is up in arms about now. The most plausible item the United States could offer up in exchange for reciprocal restraint would be the U.S. Internet freedom initiative writ large, including efforts by the United States and U.S. firms to promote certain forms of speech abroad, and to enable circumvention of foreign tools of digital control. It would be a huge cost to the United States to tamp down on those activities, which have been central to its foreign policy during the last two administrations, and which in some ways define traditional U.S. foreign policy. But the costs on the other side are very high as well, and the possibility of some forms of mutual restraint should at least be explored in a serious way.

One response to this argument that I hear in conversation is some version of: “The United States should be able to have its cake and eat it too.” On this view, the United States is the strongest nation in the world militarily and economically, and should not have to give up any of its cyber and related capabilities in exchange for relief from adversary cyber and related actions. We have to get tougher, act more aggressively, and the like. I am surprised by this reaction because in other contexts—most notably, nuclear weapons—the United States perceived a clear advantage from giving up offensive capabilities in exchange for the threat reduction of reciprocal concessions. But in any event, the “tough guy” line of thinking is belied by events of the last five years or so, which has made clear that problems of attribution, escalation, and digital vulnerability mean that no matter how powerful we are at the moment, we cannot in fact have our cake and eat it too in this context.

### Solvency---Comparative---2NC

#### Mutual agreement is a prerequisite to solvency---retaliation fails because adversaries think the US is too strong.

Jack Goldsmith 10. Teaches @ Harvard Law School and is on the Hoover Institution's Task Force on National Security and Law. "Can we stop the global cyber arms race?". 2-1-2010. https://www.washingtonpost.com/wp-dyn/content/article/2010/01/31/AR2010013101834.html

In a speech this month on "Internet freedom," Secretary of State Hillary Clinton decried the cyberattacks that threaten U.S. economic and national security interests. "Countries or individuals that engage in cyber attacks should face consequences and international condemnation," she warned, alluding to the China-Google kerfuffle. We should "create norms of behavior among states and encourage respect for the global networked commons."

Perhaps so. But the problem with Clinton's call for accountability and norms on the global network -- a call frequently heard in policy discussions about cybersecurity -- is the enormous array of cyberattacks originating from the United States. Until we acknowledge these attacks and signal how we might control them, we cannot make progress on preventing cyberattacks emanating from other countries.

An important weapon in the cyberattack arsenal is a botnet, a cluster of thousands and sometimes millions of compromised computers under the ultimate remote control of a "master." Botnets were behind last summer's attack on South Korean and American government Web sites, as well as prominent attacks a few years ago on Estonian and Georgian sites. They are also engines of spam that can deliver destructive malware that enables economic espionage or theft.

The United States has the most, or nearly the most, infected botnet computers and is thus the country from which a good chunk of botnet attacks stem. The government could crack down on botnets, but doing so would raise the cost of software or Internet access and would be controversial. So it has not acted, and the number of dangerous botnet attacks from America grows.

The United States is also a leading source of "hacktivists" who use digital tools to fight oppressive regimes. Scores of individuals and groups in the United States design or employ computer payloads to attack government Web sites, computer systems and censoring tools in Iran and China. These efforts are often supported by U.S. foundations and universities, and by the federal government. Clinton boasted about this support seven paragraphs after complaining about cyberattacks.

Finally, the U.S. government has perhaps the world's most powerful and sophisticated offensive cyberattack capability. This capability remains highly classified. But the New York Times has reported that the Bush administration used cyberattacks on insurgent cellphones and computers in Iraq, and that it approved a plan for attacks on computers related to Iran's nuclear weapons program. And the government is surely doing much more. "We have U.S. warriors in cyberspace that are deployed overseas" and "live in adversary networks," says Bob Gourley, the former chief technology officer for the Defense Intelligence Agency.

These warriors are now under the command of Lt. Gen. Keith Alexander, director of the National Security Agency. The NSA, the world's most powerful signals intelligence organization, is also in the business of breaking into and extracting data from offshore enemy computer systems and of engaging in computer attacks that, in the NSA's words, "disrupt, deny, degrade, or destroy the information" found in these systems. When the Obama administration created "cyber command" last year to coordinate U.S. offensive cyber capabilities, it nominated Alexander to be in charge.

Simply put, the United States is in a big way doing the very things that Clinton criticized. We are not, like the Chinese, stealing intellectual property from U.S. firms or breaking into the accounts of democracy advocates. But we are aggressively using the same or similar computer techniques for ends we deem worthy.

Our potent offensive cyber operations matter for reasons beyond the hypocrisy inherent in undifferentiated condemnation of cyberattacks. Even if we could stop all cyberattacks from our soil, we wouldn't want to. On the private side, hacktivism can be a tool of liberation. On the public side, the best defense of critical computer systems is sometimes a good offense. "My own view is that the only way to counteract both criminal and espionage activity online is to be proactive," Alexander said last year, adding that if the Chinese were inside critical U.S. computer systems, he would "want to go and take down the source of those attacks."

Our adversaries are aware of our prodigious and growing offensive cyber capacities and exploits. In a survey published Thursday by the security firm McAfee, more information technology experts from critical infrastructure firms around the world expressed concern about the United States as a source of computer network attacks than about any other country. This awareness, along with our vulnerability to cyberattacks, fuels a dangerous public and private cyber arms race in an arena where the offense already has a natural advantage.

Everyone agrees on the need to curb this race by creating proper norms of network behavior. But like Clinton, U.S. cybersecurity policymakers are in the habit of thinking too much about those who attack us and too little about our attacks on others. Creating norms to curb cyberattacks is difficult enough because the attackers' identities are hard to ascertain. But another large hurdle is the federal government's refusal to acknowledge more fully its many offensive cyber activities, or to propose which such activities it might clamp down on in exchange for reciprocal concessions by our adversaries.

### Solvency---Cyber Treaty---2NC

#### Cyber treaty solves attacks and miscalculation.

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/

While these frameworks provide evidence of common interests, they are indeed only a start, due to their non-binding nature. Stepping out of the laws of war rhetoric, the most ambitious and probably the most productive approach to cyber threats would be to push toward the framing of a cyber-specific treaty. A cyber-treaty would mitigate some of the outstanding challenges the DNC hack has illustrated. It would help preventing the expansion of cyber-attacks falling below the threshold in which the laws of war kick in; as importantly, it would help protect democratic political processes and domestic self-government at home and abroad.

Towards a Cyber-Specific Treaty

A treaty specific to cyber operations is no novel idea. The treaty approach was not adopted because the United States did not want to limit its rich and multifaceted cyber-interventions abroad. But a failure to pursue a treaty framework will likely come at the US’s own peril. Not only the US, but also Russia and China have become major players in this field. If one wishes to limit the damage the three can impose on each other, some agreement is required. Perhaps even merely negotiating a cyber-treaty has some value. Such a process highlights controversies and disagreement; at the same time, it “limits the arms race and paves the way to peace.”

Back in 2012, Russia sought to conclude a treaty. At that time, Vladislav P. Sherstyuk, deputy secretary of the Russian Security Council, laid out what he described as Russia’s “bedrock positions” on disarmament in cyberspace. Russia’s proposed treaty was modeled on the Chemical Weapons Convention (CWC). Russia proposed that such treaty “would ban a country from secretly embedding malicious codes or circuitry that could be later activated from afar in the event of war.” This emphasis was likely motivated by a desire to rebuke the US and Israel for the famous Flame and Stuxnet malware that infiltrated Iranian nuclear facilities’ computer systems in 2010.

As Mary Ellen O’Connell and Louise Arimatsu explained in a report from the same year, the US’s resistance to proposals for a treaty may have related to:

“US plans to use the Internet for offensive purposes […] U.S. officials claim publicly that Cyber Command is primarily defensive, but the reluctance to entertain the idea of a cyberspace disarmament treaty is raising questions about the true U.S. position.”

In 2015, Russia and China signed a pact that includes a pledge not to hack each other, as well as provisions on law enforcement cooperation and exchange of cybersecurity technologies. While Russia failed to get the US to agree on basic cyber-security principles, the two other super-powers moved forward bilaterally.

To be sure, Russia’s good intentions are nothing that we can opine about (as we do not attempt to determine Obama’s intentions). However, even if the commitment to the new cyber-specific treaty is merely a matter of optics, it may seriously help reducing risks. To understand how that might work, consider the wisdom of Sherstyuk’s appeal to the CWC in particular.

The Chemical Weapon Convention (CWC) Model for a Cyber-Treaty

The CWC is a 1997 arms-control convention, originally signed by 95 nations (188 as of today). Signatories pledged to eliminate chemical weapons, their production facilities, as well as refrain from using chemical weapons under any circumstances. The CWC also requires states to adopt measures to implement the treaty. Signatories are required, for example, to legislate statutes that penalize activities contrary to the provisions of the treaty. Finally, the CWC establishes the Organisation for the Prohibition of Chemical Weapons (OPCW), which oversees the adherence to the convention by carrying out inspections in the territory of State parties. The establishment of the OPCW is truly the most revolutionary aspect of the CWC.

The OPCW provides assistance to state parties. Among other work, it engages in advocacy promoting the abolition of chemical weapons, and provides assistance in the peaceful use of chemistry. In 2014, the OPCW led the collection and elimination of Syrian chemical weapons. While this operation has not clearly eliminated the threat of chemical weapons in Syria, it certainly played an important role.

This could also be applicable to cyberspace. A cyber-treaty based on the CWC, would establish an independent organization to monitor trans-boundary cyber activities, assist with real-time ongoing cyber-attacks, and provide intelligence to attribute cyber operations to a particular actor. This will be challenging, as cyber-security is one of the most sensitive and classified parts of contemporary national security. However, a treaty-based organization could opt for a representative structure and decision-making processes that will protect its work from being monopolized by any one super-power. Such an organization will also provide training to officials of state parties that do not have the knowledge or the means to acquire cyber security training.

The authority of the Organization will be naturally limited, but serious violations may be submitted to the United Nations, whether the General Assembly, or in more serious cases, the Security Council. The CWC rests on these assumptions. They should also be incorporated in the cyber-treaty.

The CWC requires states to legislate appropriate laws to comply with the stipulations of the Convention. A more recent example relevant to cyberspace is the 2001 Council of Europe Convention on Cyber Crime, which requires states to adopt specific laws prohibiting illegal access, data interference, computer related fraud, and more.

This model would work alongside the cyber-treaty intergovernmental organization, and will provide some sort of common ground for policy, since states parties will adopt similar domestic laws limiting the development and use of cyber offensive techniques. For example, the cyber-treaty could require states parties to adopt laws prohibiting private companies and individuals from developing certain offensive codes and techniques.

Finally, one of the CWC’s main purposes is to differentiate between desirable civilian uses of chemistry and the development of chemical weapons. The idea is to prevent the latter while not discouraging the former. This basic tenet too is applicable to the cyber realm, where some research and new technologies may be very beneficial.

A Few Important Caveats

To be sure, adapting the CWC model (with relevant modifications) to cyberspace will still not solve all threats and challenges. As David Koplow has shown in an important work, both the US and Russia are systematically violating key provisions of the CWC. Why would a cyber-treaty modeled on the agreement fare any better?

While key players are expected to continue to search for ways around their treaty-based duties, such a treaty will advance cyber-peace and cooperation between states. Russia has shown interest in developing such a treaty, while the US has not been particularly cooperative. Cyber offense is a two-way road. Back in 2012, Schneier explained this very clearly: “We might have an offensive advantage—although that’s debatable—but we certainly don’t have a defensive advantage.” Since the US is planning to maintain its attacks and surveillance of other states, it is likely to remain the target of similar activities. Recent events have proven that this is indeed the reality we live in.

### Solvency---Deterrence---2NC

#### Multilateral cyber treaty increases deterrence---creates defense and makes retaliation credible.

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

Benefits of an ICWC for Strategic Deterrence

In this section, I have outlined several reasons for and potential benefits of adopting an international convention to govern cyber conflict. As I alluded to in the introduction to this article, these reasons and benefits are contested by many scholars and practitioners. Before turning to address objections to an International Cyberwar Convention, however, it is worth briefly summarizing how an ICWC would serve to improve strategic cyber deterrence. At the beginning of this section, I argued that limitations of offensive cyber warfare dictate that strategic deterrence in cyberspace must be based as much on denying benefits to attackers (deterrence-by-denial) as on imposing costs via forceful retaliation (deterrence-by-retaliation) (see Lindsay 2015). By improving information-sharing, establishing best practices, and accelerating joint capacity building, an ICWC would help strengthen national cyber defenses and make national ICT systems more resilient to attack. Also, by instituting early warning mechanisms, an ICWC would lower the likelihood that cyberattacks will succeed. As such, a convention would serve to strengthen deterrence-by-denial (on collective cyber defense, see also Debar Dewar 2014, 14).

An ICWC would also improve deterrence-by-retaliation. As discussed, for cyber deterrence to work, states must be able to communicate clearly under what conditions a cyberattack will trigger a retaliatory response, and at what level. By clarifying what counts an act of cyber-aggression and what level of retaliation is deemed acceptable by the international community, an ICWC would thereby enhance states’ capacity to adopt and communicate an effective deterrent posture (see esp. Carr 2011).

When considering the benefits of an ICWC with respect to strengthening deterrence-by-retaliation, it is important to appreciate that effective retaliatory deterrence need not rest on a promise of immediate or massive reprisals. Rather, what is required is a credible promise that attackers will be eventually identified and some form of punishment dispensed. By instituting joint management and oversight over the process of attribution and reprisal, an ICWC would serve to slow down the process of retaliation. This would have several benefits. First, a lengthier and more systematic process of attribution and retaliation would reduce risks of conflict escalation by leaving time for aggressors to either prove their innocence or agree to voluntary compensation measures. Second, by introducing joint authorization of countermeasures, an ICWC would lower the costs (both political and material) of retaliation, thereby making retaliatory threats more credible. Joint authorization of countermeasures might also encourage collective sanctions against transgressors and thereby introduce an element of “extended deterrence” among parties to an ICWC. Third, international authorization of reprisals would make it feasible to widen reprisals beyond narrow retaliation-in-kind (i.e., using offensive cyber capabilities to strike back against an attacker’s information networks) to encompass a wider range of punitive measures: diplomatic, economic, and (in cases of grave assaults) military. Cross-domain retaliation is currently advocated by many cyber experts, since political and economic instruments are less sensitive to revelation than “in-kind” retaliation (Lindsay 2015, 58) and may be more potent against adversaries that lack sophisticated information networks to retaliate against (Kugler 2009). However, reliance on cross-domain retaliation would place high demands on the impartiality of attribution, lest vague cyber threats come to serve as political justification for economic sanctions (or even military strikes) against other nations. This speaks strongly in favor of delegating attribution to an independent international body.

### AT: Enforcement/Cheating/Verification---2NC

#### Verification possible---chemical and biological weapons prove---cyber is easier because attribution can happen ex-post.

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

Objection 1: The Impossibility of Monitoring and Enforcement

The perhaps most frequent objection to an international treaty governing cyber conflict is that it would be impossible to verify compliance or enforce the terms agreement (see Nye 2010; Clarke and Knake 2010; Lonergan 2016, 7–8; Schmitt and Vihul 2016, 44–45). As discussed, cyber weapons are notoriously difficult to monitor, mainly due to their dual-use nature and the fact that they are easily concealed (Nye 2015b; Singer and Friedman 2014, 127). Since states would not wish to comply unless they were sure others were complying, critics argue, any international agreement seeking to restrain states’ cyber conduct would quickly unravel.

When considering the force of this objection, the first thing to note is that problems of verification are hardly unique to the cyber domain. Take the example of chemical and biological weapons. Most precursors to chemical and bacteriological weapons have a range of domestic and industrial uses, and problems of “dual-use” (as well as a general inability to distinguish offensive from defensive R&D programs) have long plagued both the Chemical Weapons Convention (CWC) and the Biological and Toxins Weapons Convention (BCW) (see Ifft 2005). Nonetheless, these problems have for the most part been successfully addressed by a combination of highly detailed and strongly obligatory prohibitions, stringent domestic implementation and reporting requirements, intrusive international monitoring systems, and high penalties for cheating (for a discussion of the CWC, see Eilstrup-Sangiovanni 2009). So far, these institutional measures have deterred major transgressions. There is no a priori reason to assume a similar result could not be achieved in the cyber domain. In fact, the challenge of monitoring compliance may in some ways present a lesser obstacle to cooperation in the cyber domain than in the realm of “traditional” nuclear and bio-chem weapons. Consider that the need for reliable verification of compliance with a cyberwar convention arises not ex ante with respect to weapons development and possession, but rather ex-post with respect to weapons use. This makes an important difference. Due to the enormous and irreparable damage that can be wrought by a single nuclear strike, the bilateral treaties that dominated Cold War nuclear arms control focused primarily on restricting the development and possession of nuclear weapons and their means of delivery. By contrast, verifying and attributing the use of nuclear weapons was never a concern. Once a nuclear weapon is launched, there can be little doubt as to “who did it”; the only relevant question is whether a victimized state has the capacity to retaliate. The ability for states to monitor build-ups of offensive capabilities is thus vital to nuclear arms control.

Cyber weapons present a different problem. Since a cyberattack is unlikely to cause as widespread or irreversible damage as a nuclear attack, and since the ability of a victimized state to retaliate is unlikely to depend on the speed with which a counter-attack can be launched (or even on the ability to retaliate in kind), the main concern is not to monitor other states’ possession of offensive cyber weapons (which would admittedly be close to impossible). Instead, the thornier problem is to establish, ex post, who is responsible for an attack and decide how to respond. A joint attribution mechanism overseen by an international authority would greatly improve states’ individual and collective ability to decide such questions and would thus go a long way towards solving the problem of monitoring and enforcement.

### AT: Delay---2NC

#### Negotiation alone solves.

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

Objection 2: An ICWC Would Take Too Long to Negotiate

A second objection to a formal treaty is that it would take too long to negotiate. According to Finnemore (2011, 93), “negotiating treaties can be a slow and cumbersome process, ill-suited to fast-changing issues like cyber security and Internet governance”. Negotiating the UN Convention on the Law of the Sea took more than a decade, she observes. One might add that negotiations over the CWC, signed in 1993, spanned several decades.Footnote32 It is important to note, however, that whereas negotiations over UNCLOS and the CWC took many years, in both cases, elements of norm gestation and informal cooperation kicked off early in the negotiation process as individual states sought to gradually bring their behavior into line with emergent international norms. Indeed, experience from these and other international treaty negotiations (such as the negotiations of the International Landmine Ban Treaty) suggest that while international norm creation and acceptance is generally a slow process, the process is often accelerated by formal treaty negotiations which add political weight and visibility to an issue. While the road to a binding international agreement on cybersecurity may be long, embarking on negotiations might therefore by itself have a positive impact.

### Say Yes---Cyber Non-Intervention---2NC

#### They both say yes to cyber “non-intervention”---solves the case through a cyber “no first strike.”

Tom O'Connor, Naveed Jamali, and Fred Guterl 6/18/21. Tom O'Connor, award-winning senior writer of foreign policy at Newsweek. Naveed Jamali, Newsweek editor at large; former FBI double agent. Fred Guterl, Special Projects Editor at Newsweek. "Will Putin's hackers launch a cyber Pearl Harbor—and a shooting war?". Newsweek. 6-18-2021. https://www.newsweek.com/2021/07/09/will-putins-hackers-launch-cyber-pearl-harbor-shooting-war-1601791.html

Prospects for a Treaty

Judging from his rhetoric, Putin seems amenable to an agreement to rein in the cyber warfare shenanigans. In September, he asserted that "one of today's major strategic challenges is the risk of a large-scale confrontation in the digital field," as conveyed to Newsweek by the Russian embassy in Washington.

Putin wants to establish high-level communication between Washington and Moscow on "international information security," using existing agencies that deal with nuclear and computer readiness. He is also in favor of establishing new rules along the lines of U.S.-Soviet agreements on avoiding maritime incidents and mutual "guarantees of non-intervention into internal affairs of each other."

In a reference to the nuclear weapons that dominated the Cold War discourse on arms control, Putin is also seeking a global agreement on "no-first-strike" rules regarding cyber attacks against communications systems, the embassy said.

Sullivan told reporters that nuclear talks remained the "starting point" for bilateral discussions with Russia on cyber: "Whether additional elements get added to strategic stability talks in the realm of space or cyber or other areas, that's something to be determined as we go forward." Indeed, the joint statement on "strategic stability" released by both sides after the meeting stuck strictly to nuclear arms, with no references to cyber weapons.

Still, the talks made some progress on cyber warfare. While the Biden administration has drawn no direct link between the recent ransomware assault and the Kremlin, U.S. officials have called on Russia to hold hackers within its borders accountable for any attacks that originate there. Putin said during an interview with the Rossiya-1 outlet that he would agree to the extradition of those arrested in Russia if the U.S. does the same; Biden has vowed to reciprocate in the event such attacks were launched from U.S. soil.

In some ways, the Biden-Putin summit sends a signal that cyber warfare has taken its place alongside other military technologies as an accepted part of a nation's arsenal—and one that requires international agreements to keep in check. It also underscores the crucial importance of information technology to national defense.

### Say Yes---Cyber---2NC

#### Russia will say yes---they want to consult over cyber

TASS 20. "Russia invites US to discuss rules in cyberspace — diplomat". https://tass.com/politics/1123383

MOSCOW, February 25. /TASS/. Russia is interested in forging bilateral agreements with the United States on how to co-exist and interact in cyberspace, Russian Special Presidential Envoy for International Cooperation in Information Security Andrei Krutskikh told the Kommersant daily.

"Russia is always open for dialogue on the pressing issue of cybersecurity with any partner, including the United States. This year, we noticed certain positive signals coming from the US side, with regard to its readiness to somehow start a dialogue with Russia irrespective of the domestic political situation. The newly appointed US Ambassador to Moscow John Sullivan was among those who recently voiced ideas of this kind," the Russian diplomat said.

According to Krutskikh, Moscow welcomes this approach and calls upon its partners in Washington to "restore a normal, de-politicized dialogue on global information security between Russia and the United States."

"What we need is not attempting to change each other’s political views, but to sit at the negotiating table and agree on how we co-exist and interact in the information space. Issues on our present-day agenda are absolutely pressing, including confidence-building measures in cyberspace and efforts against cyber-terrorism and cyber-fraud," the high-ranking Russian diplomat said.

### AT: Say No---Papp---2NC

#### Politics don’t mean countries say no.

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

Opening a discussion about setting boundaries for cyber activity going forward, however, need not be seen as weakness or folly. It is precisely when bilateral relations are plumbing new depths, and there seems to be no hope for improvement, that our professional national security establishments must engage. Domestic political considerations are currently the most daunting challenge for such negotiations—in both countries. Coming to the table to reduce the risks of further and potentially catastrophic cyber miscalculations must take precedence among policymakers on both sides that value our shared future. Starting on the path to a cyber treaty is an ambitious but not unthinkable goal.

### AT: Say No---Differences---2NC

#### Differences are surmountable AND dialogue is key

Geoff Van Epps 13. Geoff Van Epps is a lieutenant colonel in the US Army. Former Senior Fellow at the George C. Marshall European Center for Security Studies in Garmisch, Germany, from 2012-2013. "Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain". The Quarterly Journal. http://connections-qj.org/article/common-ground-us-and-nato-engagement-russia-cyber-domain

Although Russia possesses an advanced capability that ranks among the best in the world, its fundamental understanding of cybersecurity diverges widely from that of the U.S. and NATO,[108] which creates philosophical and conceptual differences that pose real—albeit surmountable—obstacles to constructive dialogue on cyber issues. At present, a lack of common understanding makes any discussion between Russia and the West on cyber topics, in the words of one expert, an act of “mutual incomprehension and apparent intransigence.” [109] These differences must be understood and resolved for cooperation to bear fruit, which can only be achieved through regular dialogue and consistent interaction, a perspective reflected in the comment by the U.S. Secretary of State’s Coordinator for Cyber Issues Christopher Painter that “We need to engage with countries around the world, even with those with whom we disagree.” [110]

#### The aff is a point of agreement and differences are NOT irreconcilable

Geoff Van Epps 13. Geoff Van Epps is a lieutenant colonel in the US Army. Former Senior Fellow at the George C. Marshall European Center for Security Studies in Garmisch, Germany, from 2012-2013. "Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain". The Quarterly Journal. http://connections-qj.org/article/common-ground-us-and-nato-engagement-russia-cyber-domain

Rather than support the Budapest Convention, Russia has emphasized the need for a new international regime that more closely corresponds to its views on cybersecurity. Russian officials and academics consistently espouse a position that existing international law is inadequate and that new accords are necessary to affirm national sovereignty and deter aggressive behavior in cyberspace.[121] Their proposals, including the 2011 letter to the UN Secretary-General it co-authored with China, Tajikistan, and Uzbekistan, generally seem to share three aims: to constrain or limit competing U.S. initiatives to develop norms in cyberspace, which they view as a means of consolidating the U.S. competitive advantage in cyberspace; to affirm the rights of countries to monitor and control the flow of information over the Internet, which they see as essential to ensuring domestic security; and to prevent the further development or proliferation of offensive cyber weapons. These tenets contrast sharply with the Western emphasis on commitment to the free flow of information, measures to combat cyber crime, and state responsibility for Internet activity occurring within a country’s borders.[122] These differences might appear to be irreconcilable at first blush, limiting the odds of achieving consensus on an international framework for cyber operations.[123] However, there are many points of agreement that provide a starting point for cooperation – on securing supply chains, protecting critical infrastructure, sharing information on threats, and combating Internet use by drug traffickers and pedophiles.[124]

### AT: Say No---No Incentives---2NC

#### Technical expertise provides incentives to join a treaty.

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

Why Would States Sign Up?

The perhaps strongest argument against seeking a formal treaty to govern international cyber conflict is that the insistence on binding rules will mean that only a small group of highly committed states are willing to sign on. Yet, if designed according to the principles and purposes outlined in this article, an ICWC would in fact offer a wide range of incentives for states to come on board. To begin, intelligence-sharing and a joint mechanism for attribution as outlined above would constitute important carrots for many states, as would access to technical assistance and funding to help improve national cyber defenses. One could imagine creating additional inducements to participation, such as joint disaster response. For example, a convention could oblige states to assist other parties if they came under severe cyberattack.Footnote36 Similarly, one could envisage a multilateral fund for recovery and reconstruction which would provide financial assistance and expertise to help states repair and rebuild critical infrastructure after a cyberattack. In this regard, we can look to existing arms control treaties as a model. The CWC provides various forms of emergency assistance to state parties and establishes a voluntary fund for “Assistance and Protection against Chemical Weapons”.Footnote37 The Technical Secretariat also helps to improve national protection against chemical attacks by delivering detection equipment and alarm systems, protective equipment, and technical assistance to state parties.Footnote38 Together with active support for compliance, these provisions have provided an important incentive for states to participate. Similar provisions in the cyber domain could serve to encourage buy-in by reluctant states.

### AT: Internet Freedom DA---2NC

#### Internet freedom doesn’t solve human rights.

Alberto J. Cerda Silva 13. An assistant professor of computer law at the University of Chile. He is a founding member and director of international affairs of the NGO Derechos Digitales. He is currently a Fulbright Scholar pursuing doctoral studies at Georgetown University Law Center with a thesis on human rights and Internet regulation in Latin America. "Internet Freedom is not Enough". Sur - International Journal on Human Rights. https://sur.conectas.org/en/internet-freedom-not-enough/

Internet Freedomis a partial approach to the importance of the network from a human rights perspective, since it is only limited to freedom of expression and the right to privacy. It is implausible to suppose that the contribution and potential of the Internet for the realization of other human rights could still be disclaimed, but Internet Freedom does not pay attention to more than a couple of them, those that best reflect a nineteenth-century liberal conception of the State.

Internet Freedom does not include any mention of economic, social, and cultural rights. In this way, improving the accessibility for those without access is not a priority for Internet Freedom, even if it contributes to the reinforcement of democracy, individual and collective development, and the realization of other rights. It also omits the Internet’s role in the preservation and promotion of cultural and linguistic identities, particularly considering the abrasive effects of the unidirectional flow of information from a small number of countries to many others.

#### Non-unique---Internet freedom down now.

Ina Fried 21. author of Axios Login. “Internet freedom declines for 11th year in a row.” https://www.axios.com/2021/09/21/internet-freedom-declines-11th-year

An increase in network shutdowns, combined with a rise in disinformation campaigns, adds up to another decline in internet freedom in the U.S. and around the globe, according to Freedom House.

Why it matters: It's the 11th consecutive year that the internet has been less free globally and the fifth straight yearly decline in the U.S., the group says in its annual report on the subject.

Among the findings:

Authorities in at least 48 countries aimed to enact new rules for tech platforms over the past year.

* The greatest declines in internet freedom over the last year took place in Myanmar, Belarus and Uganda.
* More countries arrested people for nonviolent political, social or religious speech last year than in any previous year.
* As we've reported, partial or complete internet shutdowns are on the rise and are also increasingly costly to the global economy.