A Cyber Warfare Convention? Lessons from the Conventions on Chemical and Biological Weapons

Cameron S. Brown and David Friedman

Dozens of states are currently locked in a cyber arms race. Few countries divulge their total annual investment in either offensive or defensive cyber warfare capacities, but there is little doubt that for most governments the overall growth in both financial and personnel investment has been exponential.[1] This increased cyber investment is underway for several reasons, but most importantly because cyber warfare capacities have matured into terribly potent weapons. Far beyond low level disruption of websites (e.g., distributed denial-of-service, or DDoS, attacks) or viruses that turn one's computer into a spam-generating satellite office for some "Nigerian prince" desperately seeking to recover his inheritance or other such scam, complex cyber weapons such as the infamous Stuxnet and Flame have allowed states to conduct pinpoint strikes and wide scale espionage on an impressive range of military, diplomatic, and industrial targets.[2] These attacks are now conducted with great effectiveness and substantial deniability, and for several years have even been able to penetrate systems that are "air-gapped" – i.e., totally disconnected from the internet.[3]

This newest revolution in military affairs has led dozens of military powers to incorporate cyber weapons into their order of battle at both the strategic and tactical levels. On the strategic level, Russia's cyber attacks (routed via a Brooklyn-based server) disabled Georgian infrastructure at the outset of their 2008 war, and the United States reportedly possesses the cyber capacities to shut down the entire air defense systems of some adversaries even before the first American plane ever leaves the runway.[4] On the tactical level, American cyber weapons specialists are now integrated

into regular combat units, even against relatively low-tech opponents such as the Taliban in Afghanistan.[5]

During peacetime as well, intelligence organizations employ cyber weapons at a dizzying pace. The Chinese are presumed to have hacked into almost every major institution in Washington and have collected so much information that their biggest intelligence hurdle these days is just sifting through and analyzing the billions of documents they have collected.[6] Indeed, one recent estimate (of admittedly questionable methodology) put the damage of cyber espionage to American businesses alone at over $300 billion per year, roughly equivalent to all annual US exports to Asia. The Commander of the United States Cyber Command and Director of the National Security Agency, General Keith Alexander, deemed this theft of intellectual property (IP) as "the greatest transfer of wealth in history."[7]

With industry and military secrets being stolen wholesale, and with vast amounts of critical military and civilian infrastructure so vulnerable to attack, many public figures have called for a convention on cyber warfare (separate from the one on cyber crime).[8] In September 2011, the Russian Ministry of Foreign Affairs, along with China, Tajikistan, and Uzbekistan, went so far as to submit a draft convention to the United Nations General Assembly for consideration as a resolution.[9] At a conference in May 2012, Eugene Kaspersky, founder of the anti-virus software company Kaspersky Labs, argued that hacker groups (like Anonymous) could use cyber weapons like Stuxnet against other countries by copying code and utilizing it in their own future attacks on a country's electrical grids, telecommunications networks, and financial or governmental institutions. Therefore, he concluded, "I'm afraid that there's only one way that they can be protected and that's international agreements against cyber weapons, same as was done with nuclear weapons, chemical weapons and biological weapons."[10]

Although many American officials have expressed skepticism about prospects for such a convention, several have been in favor, including Senator Dianne Feinstein (D-Calif.), Chairman of the Senate Intelligence Committee. In a short statement on the subject, she said that "robust diplomatic efforts should be made with the goal of effecting international agreements among key actors regarding cyber behavior. The time has come to look at the value of a cyber treaty with built-in mutual assurances of behavior."[11] Among the most important American proponents of a cyber convention is Richard Clarke, who authored the book *Cyber War* and who served three presidents

as National Coordinator and Special Assistant for Counterterrorism, Security, Global Affairs and Cyber Warfare. During a speech at the Naval Postgraduate School on August 17, 2010, Clarke summarized an argument from his book:

> We also need to think seriously about an arms control treaty for cyberspace…because two, and more, can play this game. Between 20 and 30 countries now have cyber warfare commands…. It [an arms control agreement] won't be easy – attribution [determining who is behind an attack] is immensely difficult, so the cyber world doesn't lend itself to deterrence strategies like mutually assured destruction with nuclear weapons – but we have to try, just as we did with conventional weapons and bio weapons. We succeeded with those, and the only way to get there is by starting…. Most countries would agree to sign a treaty not to attack each other's international financial and banking system networks. They don't want to cross that Rubicon, or the entire international banking system could go down. We have an international regime for cyber crime, and we need one for cyber war – to rule out some things globally. But we have to take this seriously and move quickly. If we're not careful – if we don't take cyber defense and cyber arms control seriously – we may find ourselves in a shooting war and wake up to find that the enemy has pulled the plug on all our shiny, trillion dollar weapons, that our chips and supply chains have already been compromised, that our pipelines have been shut down and our trains derailed, all while our computer screens are telling us that nothing is happening.[12]

Calling for a convention on cyber warfare may be popular, but could such a convention ever actually be enacted? Moreover, even if such a treaty comes into force one day, would signatories abide by it? (The two questions are analytically distinct, as politicians could have incentives to sign an agreement to which they do not intend to adhere.) In this realm, there is healthy reason for skepticism. For instance, if a dependable verification mechanism is at the heart of any arms control convention, then cyber warfare is a terrible candidate. Arms control regarding nuclear weapons, for instance, has generally been quite successful, in large part because developing these weapons requires a number of large warehouse-sized facilities filled with

radioactive material, thousands of white lab coat-wearing scientists and engineers, and usually the import of special machinery and materiel. An advanced cyber warfare base, on the other hand, could in many ways be observationally equivalent to a college dormitory.[13]

Precisely for these reasons, proponents of a cyber convention like to point to the biological and chemical weapons conventions (BTWC and CWC, respectively), both of which were meant to restrict the development and use of weapons whose verification challenges are almost as difficult as their cyber counterparts. This paper considers that analogy seriously. First, it considers what lessons a cyber convention could gain from the experiences of the four main treaties that have forbidden chemical and biological weapons: Hague, Geneva, BTWC, and CWC. It then addresses the question of whether there are critical differences between chemical or biological weapons and their cyber counterparts that might undermine the analogy altogether.

The Origins of Chemical and Biological Arms Control

Although typically classified as weapons of mass destruction, biological and chemical weapons (BW and CW, respectively) considerably predated nuclear and radiological weapons, and their initial use dates back to antiquity. In India, toxic fumes were used as weapons as far back as 2000 BCE, and in 400 BCE, the Spartans are said to have used wood saturated with pitch and sulfur during sieges to choke city defenders. In 1346, in what is now Fedossia, Ukraine, bodies of Tartar soldiers who had died of the plague were catapulted over the walls and into the besieged city.[14]

When countries first sought to alleviate the "the calamities of war,"[15] among the first restrictions countries accepted were prohibitions against the use of poison munitions. In preparing the field manual for the Union Army in 1863 at the behest of President Lincoln, Francis Lieber wrote, "Military necessity does not admit of cruelty... It does not admit of the use of poison in any way." A decade later, Czar Alexander II convened a convention in Brussels where delegates from 15 countries considered a draft agreement that would set out "laws and customs of war." Among the very specific prohibitions was the rule forbidding the "employment of poison or poisoned weapons" (Article 13). Though not ratified at the time, this document served as the basis of the Hague Conventions of 1899 and 1907, which went even further and prohibited the "diffusion of asphyxiating or deleterious gases" (Declarations IV, 2).[16]

These agreements proved worthless during World War I, as Germany, France, and England made wide use of CW, killing over 100,000 and injuring over a million soldiers.[17] In light of both the wide scale use of chemical weapons and the massive bloodshed overall, post-World War I leading countries signed a number of international agreements, such as the Covenant of the League of Nations and the Kellogg-Briand Pact of 1928. These agreements ultimately aimed at ending war, but in the event that war proved unavoidable, the goal was to attenuate its worst excesses. The Geneva Convention of 1925 specifically prohibited the use of chemical and bacteriological weapons in war.

Given CW's widespread use in World War I, it is curious that they were barely used on the battlefield during World War II. To be sure, commitments to the Geneva Convention did not prevent the Axis powers from using CW.[18] The Germans killed millions in their gas chambers, Mussolini's forces had used CW in Ethiopia only a few years before, and the Japanese actually began using CW and BW in China in the early 1940s.[19] Instead, what deterred the Axis powers from using CW were several unambiguous Allied threats – red lines, as it were – that employing CW anywhere would be met, as President Roosevelt put it, with "retaliation in kind and in full measure...We shall be prepared to enforce complete retribution."[20] Incorrectly believing the Allies possessed superior CW armaments, the Axis powers were deterred for the rest of the war.[21]

Chemical and Biological Weapons Proliferation after World War II

Although not widely utilized on the battlefield during any Cold War proxy war,[22] BW and CW were incorporated into the American and Soviet strategic arsenals. The United States and the Soviet Union, and later France and England, developed and maintained large quantities of different varieties of chemical and biological weapons. By 1960, over a dozen countries pursued or possessed CBW, including Western democracies like Australia, West Germany, and Sweden; the Eastern bloc countries of Czechoslovakia and Yugoslavia; and others, including Egypt and China.[23]

In the 1960s, several additional Soviet client states, including Cuba, East Germany, and North Korea, began CW arsenals. During the 1970s and 1980s, dozens of additional countries, mostly developing or poor countries, made efforts to attain CW or BW – either indigenously or via foreign suppliers.[24]

These countries saw CW and BW as a substitute for nuclear weapons ("a poor man's bomb"), as they required far less investment and technological sophistication. BW and CW were also thought to increase a country's deterrence and mitigate an opponent's conventional advantage.[25]

Nowhere was CW and BW proliferation more rampant than in the Middle East. Numerous states, including Egypt, Iraq, Syria, Iran, and Libya, made great efforts to acquire BW and CW, as well as advanced delivery systems like long range ballistic missiles, in order to maintain some measure of strategic deterrence against each other and an allegedly nuclear Israel. Most importantly, all five occasions where states used nonconventional weapons since World War II occurred in the region: Egypt employed CW during the civil war in Yemen in the early 1960s; Libya used CW in Chad in 1987; and Saddam Hussein used it in the 1980s, first against Iran and then to suppress the Kurdish rebellion in Iraq. Finally, the Assad regime used CW approximately a dozen times against rebel-held areas during the Syrian civil war.

Recently, several terrorist organizations have attempted to develop or acquire CW or BW, precisely because chemical and biological weapons suit the modus operandi of terror organizations: they instill fear, panic, and demoralize their adversary, even if (like terrorism in general) they kill few people in absolute terms. Indeed, although several terror organizations (e.g., al-Qaeda) declared their willingness to use CW and BW, few groups have been able to develop either indigenously, and only in three instances has either weapon actually been employed.[26] Indeed, if anything, those incidents mostly demonstrated the terribly limited effectiveness of CW and BW at killing people when wielded by amateurs. In fact, even the Japanese cult Aum Shinrikyo, which used sarin gas in the Tokyo subway system in 1995 (the only time terrorists have used CW), decided to abandon its plans to use biological agents because they are so difficult to disperse effectively, not to mention to develop and deploy without infecting oneself.[27]

Post World-War II Arms Control Efforts

Over the past 40 years, states have sought to strengthen the Geneva Convention of 1925 by forging more binding and detailed arms control and nonproliferation regimes (both at the regional and global levels). Interestingly, many countries gave up their BW and CW programs unilaterally.

Unilateral Actions

During the 1960s and 1970s, several countries took unilateral steps to eliminate their stockpile of biological weapons. In 1969, President Nixon ordered the elimination of all biological weapons stockpiles, and halted all research, development, and production of BW. Once they became nuclear states, Britain and France also abandoned their programs.[28] In 1974, roughly half a dozen countries, including Australia, Sweden, Austria, Cuba, and East and West Germany, also unilaterally ended their CW programs. Countries undertook these unilateral decisions for different reasons, including the ethical belief that because these weapons are indiscriminate and potentially catastrophic, their use is immoral.

Generally, however, there were also several critical strategic motivations. First, BW and CW require an intensive investment, especially to store safely and in a manner that ensures battle-readiness. Second, although even very small amounts of BW can achieve the high level of toxicity required, effectively employing BW or CW on the battlefield is always fraught with great uncertainty, as variations in weather, wind, and sun radiation will have a dramatic effect on agent survival and contagion rates. Third, once used, many agents cannot be limited to a small, controlled target area, and under certain conditions, could come back to haunt the user as well (especially regarding certain BW agents). Finally, the deterrence value of these weapons is questionable as well. On the one hand, neither is likely to deter against nuclear weapons, since their raw destruction can in no way compare to the potential of nuclear weapons. Furthermore, the effect of BW is not immediate, with casualties only appearing a day or two after contamination, and with both BW and CW, victims can often be treated. On the other hand, capacity to respond "in-kind" to a CW or BW attack is not optimal for a nuclear weapons state, which could otherwise credibly threaten to retaliate against a CW or BW attack with a nuclear strike. In other words, for some countries, a CW or BW arsenal may even undermine its deterrence.[29]

Finally, it is significant that while some countries decided unilaterally to forego biological and chemical weapons, these countries maintained and even strengthened their defense capabilities. Disarming countries understood that some countries will continue to arm themselves with chemical and biological weapons clandestinely, and that defense capabilities increase deterrence against a potential attacker.

The Biological and Toxin Weapon Convention (BTWC)

The BTWC was opened for signature in April 1972 and came into force in 1975. In several ways, the BTWC was a turning point in the field of arms control and nonproliferation as the first treaty to ban the development, production, and storage of an entire category of weapons of mass destruction (WMD); the aforementioned Geneva Convention only outlawed WMD use. As opposed to the NPT, the BTWC was an egalitarian treaty, binding every signatory to the same standards. The treaty is also noteworthy for having been signed during the height of Cold War suspicion between the USSR and the US. Yet as a consequence of this mistrust, the signatories could not agree to verification mechanisms for the BTWC, meaning that the treaty's main value is declarative.

The BTWC has an inherent and unresolvable tension, in that the research and development of biological agents for the purpose of improving defense capabilities and public health is not forbidden. On the contrary, the treaty encourages cooperation and the transfer of technological know-how from developed to developing countries. However, it is difficult to distinguish between offensive and defensive research and development, which makes it difficult to develop a tight safeguard and verification regime. This comes on top of the usual verification challenge that any inspection regime runs the risk of exposing a state's secrets in other areas as well. Given these difficulties, efforts to create a verification and safeguard regime have so far failed.[30]

At present, 163 countries are members (i.e., signed and ratified) of the BTWC, 13 countries have signed the treaty but never ratified it, and roughly 20 states have not signed. Great efforts, both bilateral and multilateral, have been made to convince non-member states to join. Further efforts have been made to improve the treaty by including confidence building measures such as notification of plague outbreaks, notification of bio-terror exercises, and establishment of security labs. These confidence building measures could help compensate for the lack of a verification regime; however, an insufficient number of states actually comply even with these, largely out of fear of exposing valuable information. Beginning in 1994, an ad hoc group was established with the goal of creating a new, far-reaching convention based on the CWC for biological weapons, which would in effect supersede the relatively toothless BTWC. However, facing stiff opposition from the United States in particular, this attempt died in 2001 at the Fifth Review Conference when the draft text failed to achieve a consensus.[31]

The Chemical Weapon Convention

The CWC came into force in 1997, following 24 years of difficult negotiations. When drafting the CWC, negotiators attempted to incorporate lessons learned from previous experience with the NPT and the BTWC, especially regarding implementation. Much like the BTWC, the CWC is an egalitarian treaty. However, unlike the original NPT agreement and the BTWC, it has a robust and invasive verification and safeguard regime, and a clearly defined list of banned substances. The treaty bans the development, manufacturing, stockpiling, and use of chemical weapons and obligates members to eliminate all their stockpiles over a defined period of time. Members must report all stockpiling, development, and manufacturing facilities, including civilian facilities that manufacture materials listed by the treaty. Experts hold regular inspections of the declared facilities, and the treaty itself is managed by the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague, employing several hundred staff members.

The invasive verification mechanism includes a "surprise inspection" option on short notice, executed by the OPCW following a substantiated complaint by another member state. This mechanism was a source of debate during the treaty negotiation due to the sensitivity inherent in the measure. Ironically, however, to this day not a single complaint has been filed, and thus not a single "surprise inspection" has been executed. This is due to two main reasons. First, it is no simple matter to collect sufficient evidence against a suspected state to merit a "surprise inspection" by the OPCW. Second, states are concerned that once the "surprise inspection" option is used, it will open a Pandora's Box, potentially hurting them as well.

As of today, the treaty has 190 member states; two countries have signed but did not ratify (Israel and Myanmar), and four countries have not signed the treaty (Angola, Egypt, North Korea, and South Sudan).[32] There is a prevailing belief that the CWC, at least on the surface, is an arms control success story. Countries have and continue to declare facilities, as required of them. Countries eliminate large quantities of chemical weapons and substances, and regular inspections give the impression that the treaty has been successful in promoting the norms prohibiting use and proliferation of CW.

BTWC and CWC: Lessons

Thus far there is no definitive version as to what impact either the BTWC or CWC has had, as no one has yet given a reliable estimation of the counterfactual: how many states would have given up CW or BW (or never pursued them in the first place) if neither treaty was ever signed.[33] With this caveat in mind, several conclusions can be drawn from figure 1, which shows how many states possessed either weapon from 1945 until 2000.

First, neither treaty has by any means entirely eliminated the possession of CW or BW, and there are countries that have signed both treaties that are suspected of violating their obligations. Second, some countries clearly abandoned these weapons irrespective of treaty obligations, as evidenced by the fascinating trends whereby some countries gave up CW after the BTWC was opened for signing; the same is true for BW relinquishment after the CWC came into force. Such unilateral abandonment suggests that these weapons were not perceived as unequivocally useful. Finally, it is interesting that the most significant drops in global possession rates for both CW and BW occurred immediately after these treaties were first opened for signature (the NPT, on the other hand, apparently had no such effect). This trend suggests that the treaties themselves played some role, though what that role is awaits further research.

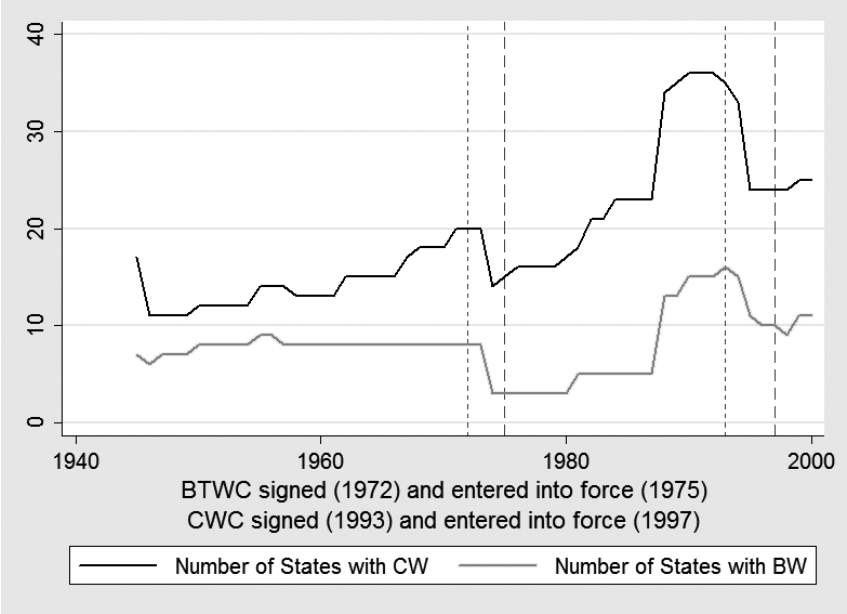

Figure 1. BTWC, CWC, and Rate of CBW Possession[34]

In this vein, caution is in order regarding any evaluation of the normative effect of these conventions on preventing the actual use of either weapon. Signing The Hague Convention of 1899 did not prevent massive use of chemical weapons in World War I. Similarly, the Geneva Convention was less important in preventing their massive battlefield use in World War II; what primarily deterred their use were overt threats of massive retaliation. Likewise, several terror organizations have openly declared that they are not bound by these taboos, but thus far have not used these weapons. Again, the lack of terrorist use suggests that the historical rarity of CW and BW use may be entirely due to considerations of effectiveness and efficiency relative to readily available conventional alternatives.

That said, it is noteworthy that the BTWC and CWC exist at all, given that both are fraught with massive verification and enforcement challenges. First, in both chemical and biological weapons, many substances and methods are "dual use" – meaning they have both legitimate civilian as well as banned military purposes. Even within military use, chemical and biological substances can be developed for offensive purposes (thus, prohibited) or permitted, and even encouraged, defensive purposes. For example, the development and manufacture of a vaccine usually requires developing a micro-organism (virus or bacteria), weakening it, and producing mass quantities in order to vaccinate the population. Using the same methods and infrastructure, one can develop an even more violent microorganism and use it as a biological weapon.

Second, particularly in biological weapons, the amount of weaponized substance needed is very small. Large development and production facilities are not needed, and it is possible to conduct research and development for offensive use in small, simple, and undetectable labs. Likewise, recent developments enable the manufacturing of chemical substances in mini-reactors that are difficult to identify. Comparatively, nuclear weapons and missiles require infrastructure and labs that are much harder to conceal.

Another relevant lesson for the cyber realm is that in the years that followed the drafting of the CWC, several countries, most notably the Soviet Union, developed highly toxic materials not covered in the treaty. These substances are now widespread, remaining outside the CWC's control mechanism, and precisely for that reason, pose a threat to the treaty.

Prospects for a Convention on Cyber Warfare

What from the experience of the CWC and BTWC relates to cyber warfare? Can a convention be reached and would all relevant actors adhere to it?

The first lesson from the BTWC and CWC is that whether effective verification is possible or not is not, as logicians would put it, a "necessary condition" for determining whether states sign and even ratify an arms control convention. Even more counter-intuitively, as indicated by figure 1, it may not even be the most important factor for determining whether countries abide by an arms control treaty. Instead, the most important lesson from the experience of the CWC and BTWC is that perception of these weapons' limited tactical and strategic utility was paramount in the willingness of some states to abandon them, and likely factored into the decision making of other states not to pursue BW or CW in the first place.

In other words, many have drawn an analogy between BW and the cyber realm because of the shared verification challenges as a way to suggest that a cyber convention is a real possibility. Yet in stark contrast to CW and BW, cyber weapons are not only already extremely effective at achieving a wide variety of aims, but programmers are still pushing the frontier by leaps and bounds as to what cyber weapons can accomplish. This is perhaps the single greatest reason why consensus is unlikely to be achieved on a cyber convention in the coming years.[35]

Of course, this does not mean that inherent obstacles to verification are unimportant to the robustness and success of an arms control regime. While on paper the BTWC and CWC take polar opposite approaches to verification – with the BTWC having almost none and the CWC having an extensive and intrusive scheme – in practice they are actually more similar than one might expect, because the CWC's challenge inspection mechanism was not used even once since the treaty came into force.

If inherent obstacles to verification matter, then cyber weapons again appear to be a one of the worst candidates for an arms control convention. If anything, the verification challenges of cyber weapons are far worse than those of CW or BW. To begin with, almost everything about an offensive cyber program is dual use (similar to a BW program, only more so). This means, for instance, that nothing a country or lab imports could even appear suspicious. The dual use problem is so overwhelming for cyber that even if an inspection team were to walk right through an offensive cyber warfare center during a short notice "snap" inspection, it would likely appear terribly

similar to most computer programming companies, and worst of all, would be indistinguishable from a defensive cyber command post. As a result, it would be nearly impossible to catch a country cheating "red-handed."[36]

Moreover, the civilian infrastructure that engages in software development is far larger than its biological or chemical counterparts, meaning pinpointing a cyber command would be like finding a needle in a haystack. Likewise, the thousands of private software companies will not be interested in having foreign arms control experts looking too closely at what they are doing, as they are more vulnerable to industrial espionage than other fields. Finally, whereas CW and BW development may be very hard to detect, the actual use is easier. When CW is used, it is relatively easy to detect as CW agents stand out from their biological environments, and so cannot be used for long and on a large scale undetected. The same, of course, is not true for cyber weapons, which often go undetected for years after being released. Likewise, while many BW agents carry genetic and other signatures so that countries can make a determination with some degree of accuracy about the origin of the weapon, cyber weapons often lack such identifying features.

Presumably another point in common, at least between BW and cyber, is that if a weapon cannot be controlled after use (i.e., there is potential "blow-back"), then states should have greater motivation to agree that the weapon not be used at all, and hence sign a convention. In its report, the EastWest Institute argued, "Cyber weapons can deliver, in the blink of an eye, wild viral behaviors that are easily reproduced and transferred, while lacking target discrimination."[37] However, critical in that determination here too is whether scientists believe they can forecast the outer limits of effectiveness and control. In other words, if a new type of weapon emerges that is difficult to contain, this does not mean it will forever be so. In the case of BW, for instance, it took decades before scientists thought they had reached a technological plateau, whereby it became difficult to imagine BW without potential blow-back concerns. Cyber weapons may have blow-back concerns, but it is entirely imaginable that once a weapon is deployed and discovered, offensive programmers can then share the vulnerabilities with those on the defensive end to plug the holes immediately. This is not true for CW or BW, certainly not with the same ease or cost.

Another major consideration is how costly or difficult is the weapon to develop and/or deploy. As the costs of development and deployment grow, fewer actors will have the wherewithal to develop, maintain, or use them.

If the costs become especially high, both non-state actors and poor states will be unable to develop or use the weapon. This is critical for a number of reasons, first, because fewer actors make verification more feasible, by reducing costs for setting up an impartial verification regime and for creating an intelligence capacity for covertly verifying compliance. Second, smaller numbers of actors should also increase the likelihood that actors will uphold their obligations, as violations of one's commitment is more likely to be met with retaliation, or at least should lead to a collapse of the agreement (which should be valued by potential violators as well). Thus as more actors can obtain and use a weapon, deterrence becomes more difficult. Again, although the costs for CW and BW development are not terribly prohibitive, they are still far greater (and the requisite skills more rare) than waging a cyber attack.

Finally, there are critical normative differences between CBW and cyber weapons. When nations in the modern era first prohibited the use of poisons and gases, they were motivated by the idea that they caused excessive and unnecessary pain and suffering, and thus had no place in the civilized world.[38] In contrast to CW and BW, however, cyber weapons are elegant in use: they achieve their aims without gruesome civilian deaths painting grisly portraits on TV screens worldwide. Indeed, they generally leave no images at all. In that case, and given that states cannot realistically be expected to stop fighting or engaging in espionage, then it is difficult to understand how a normative consideration might lead to a convention on cyber warfare when these weapons are no worse than conventional weapons, which are only rarely checked by international convention.

Notes

The authors would like to thank Daniel Cohen, Aviv Rotberg, and Gabi Siboni for their comments and thoughts about this article, and Tamar Levkovich for her dedicated research assistance. We would also like to thank Michael Horowitz and Neil Narang for giving us access to their data and paper drafts prior to publication.

1 In January 2013, the United States Department of Defense announced that its Cyber Command would grow from 900 personnel to 4,900. See Ellen Nakashima, "Pentagon to Boost Cyber Security Force," *Washington Post*, January 28, 2013, http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html. The British government spent an additional £560 million over four years, which security experts have called a relatively small sum. See Mark Urban, "Is UK Doing Enough to Protect Itself from Cyber Attack?" *BBC News*, April 30, 2013,

http://www.bbc.co.uk/news/uk-22338204. In 2012, and again in August 2013, the Russian government announced plans to set up both a cyber command of its own, as well as a Russian equivalent of DARPA that would work on advanced research projects. See "Russia Considering Cyber-Security Command," *Ria Novosti*, March 21, 2012, http://en.rian.ru/russia/20120321/172301330.html, and "Russian Army Indicates Cyber Force Plan Underway," *Ria Novosti*, August 20, 2013, http://en.ria.ru/military_news/20130820/182870107/Russian-Army-Indicates-Cyber-Force-Plan-Underway.html. One market research report claimed annual global spending is set to rise by 50 percent from 2013 to 2023. See "Cyber Warfare Systems Market Expanding to US$19.4Bn by 2023,"*Aerospace & Defense News*, August 8, 2013, http://www.asdnews.com/news-50561/Cyber_Warfare_Systems_Market_Expanding_to_US$19.4Bn_by_2023.htm.

2 On the extensiveness of cyber espionage, see, for example, Craig Timberg and Ellen Nakashima, "Chinese Cyberspies have Hacked most Washington Institutions, Experts Say," *Washington Post*, February 21, 2013, http://www.washingtonpost.com/business/technology/chinese-cyberspies-have-hacked-most-washington-institutions-experts-say/2013/02/20/ae4d5120-7615-11e2-95e4-6148e45d7adb_story.html; Sohail al-Jamea, Robert O'Harrow, Jr., and Whitney Shefte, "Zero Day: Exploring Cyberspace as a New Domain of War," *Washington Post*, June 2, 2012, http://www.washingtonpost.com/investigations/zero-day-exploring-cyberspace-as-a-new-domain-of-war/2012/06/02/gJQAFgc09U_video.html. On Stuxnet, see John Markoff, "Malware Aimed at Iran Hit Five Sites, Report Says," *New York Times*, February 11, 2011, http://www.nytimes.com/2011/02/13/science/13stuxnet.html; William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

3 On bridging air-gapped systems, see James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival: Global Politics and Strategy*, January 28, 2011, http://dx.doi.org/10.1080/00396338.2011.555586.

4 The Russian example was mentioned by Richard Clarke, a former National Coordinator and Special Assistant for Counterterrorism, Security, Global Affairs, and Cyber Warfare, in a speech at the Naval Postgraduate School on August 17, 2010. Barbara Honegger, "Former Counterterrorism Czar Richard Clarke Calls for New National Cyber Defense Policy to Prevent a Cyber 9/11," Naval Post-Graduate School website, http://www.nps.edu/About/News/Former-Counterterrorism-Czar-Richard-Clarke-Calls-for-New-National-Cyber-Defense-Policy-to-Prevent-a-Cyber-9/11-.html. On air defenses, see Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *New York Times*, October 17, 2011, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

5 For integration of cyber warriors into regular combat missions, see Tom Gjelten, "Pentagon Goes on the Offensive Against Cyberattacks," *National Public Radio*, February 11, 2013, http://www.npr.org/2013/02/11/171677247/pentagon-goes-on-the-offensive-against-cyber-attacks.

6 Timberg and Nakashima, "Chinese Cyberspies have Hacked Most Washington Institutions, Experts Say."

7 The $300b estimate and quotation come from "IP Commission Report," IP Commission, May 2013, http://ipcommission.org/report/IP_Commission_Report_052213.pdf; James A. Lewis, a senior fellow and director of the technology and public policy program at the Center for Strategic and International Studies, has taken issue with the estimate. See James Andrew Lewis, "Five Myths about Chinese Hackers," *Washington Post*, March 22, 2013, http://articles.washingtonpost.com/2013-03-22/opinions/37923854_1_chinese-hackers-cyberattacks-cold-war.

8 Some have put forward more modest proposals, like British Foreign Secretary William Hague, who in his speech to the Munich Security Conference in February 2011 suggested that the widespread threat of cyber weapons requires a "global response," whereby countries would agree to certain standards of behavior on the internet. See "William Hague: UK is under Cyber-Attack." *BBC News*, February 4, 2011, http://www.bbc.co.uk/news/uk-12371056 . Similarly, the June 2013 summit between China's President Xi Jinping and President Obama in California sought to create more informal understandings on cyber warfare and espionage between the two countries, though seemingly with little success. Alternatively, the EastWest Institute proposed ways to adapt previous conventions (e.g., Geneva Conventions) to the cyber age. See Karl Frederick Rauscher and Andrey Korotkov, "Working towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace," EastWest Institute, 2011.

9 Convention on International Information Security, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument. See also Louise Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations," in *2012 4th International Conference on Cyber Conflict*, eds. C. Czosseck, R. Ottis, K. Ziolkowski (Tallin: NATO CCD COE Publications, 2012), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6243968.

10 Lee Taylor, "Cyber Warfare Technology will be used by Terrorists, says Eugene Kaspersky," *Perth Now*, May 22, 2012, http://www.perthnow.com.au/technology/cyber-warfare-technology-will-be-used-by-terrorists-says-eugene-kaspersky/story-fn7bsj10-1226363625940. See also Andrew Colley, "Cyber Weapons Conventions Needed, Kaspersky tells CeBIT," *The Australian*, May 22, 2012.

11 Senator Feinstein's remarks, as prepared for delivery, February 2, 2010. See http://www.feinstein.senate.gov/public/index.cfm/2010/2/909a405b-5056-8059-7671-b791002862e1-post.

12 Honegger, "Former Counterterrorism Czar Richard Clarke Calls for New National Cyber Defense Policy to Prevent a Cyber 9/11." Brackets are in original article.

13 The allusion was made by Frank Langfitt, "U.S. Security Company Tracks Hacking to Chinese Army Unit," *National Public Radio*, February 19, 2013, http://www.npr.org/2013/02/19/172373133/report-links-cyber-attacks-on-u-s-to-chinas-military.

14 Jane's Defense Weekly, *Jane's US Chemical-Biological Defense Guidebook: Comprehensive Resource for Chemical and Biological Agent Weaponization and Emergency Response* (United Kingdom: Jane's Information Group Limited, 1998).

15 Declaration of St. Petersburg, November 29, 1868.

16 Historical agreements can be found at the International Committee of the Red Cross website: http://www.icrc.org/applic/ihl/ihl.nsf/vwTreatiesHistoricalByDate.xsp.

17 The website of the Organisation for the Prohibition of Chemical Weapons, http://www.opcw.org/chemical-weapons-convention/about-the-convention/genesis-and-historical-development.

18 Price and Tannenwald argue that the taboo had an important impact in preventing CW use. See Richard Price and Nina Tannenwald, "Norms and Deterrence: The Nuclear and Chemical Weapons Taboos," in *The Culture of National Security: Norms and Identity in World Politics*, ed. Peter Katzenstein (Columbia University Press, 1996), pp. 114-52.

19 On BW use, see the interview (undated) with Jeanne Guillemin, author of *Biological Weapons: From the Invention of State-Sponsored Terrorism to Contemporary Bioterrorism*, Columbia University Press, http://cup.columbia.edu/static/Interview-Guillemin-Jeanne. Regarding CW, this section benefited greatly from Frederic J. Brown's *Chemical Warfare: A Study in Restraints* (Princeton, NJ: Princeton University Press, 1968), pp. 198-240.

20 As quoted in Brown, *Chemical Warfare,* p. 201. The statement was sent to the President by the Department of State on June 3, 1942.

21 Ibid., p. 235. For two contrasting views on why the norm held in World War II, see Jeffrey W. Legro, "Which Norms Matter? Revisiting the "Failure" of Internationalism," *International Organization* 51 (1997): 31-63; and Price and Tannenwald, "Norms and Deterrence: The Nuclear and Chemical Weapons Taboos."

22 Napalm, phosphorus shells, and other weapons not classified as CW in the CWC have been used on occasion elsewhere.

23 Michael Horowitz and Neil Narang, "Poor Man's Atomic Bomb? Explaining the Relationship between Weapons of Mass Destruction," *Journal of Conflict Resolution* 57 (November 2013), online, appendix tables 1-2.

24 Twenty-three countries sought chemical weapons and ten sought biological weapons. Those who began pursuing CW in the 1970s or 1980s were: Argentina, Syria, Vietnam, Libya, Ethiopia, Taiwan, Afghanistan, Pakistan, Saudi Arabia, Angola, Iran, Brazil, Chad, Chile, Indonesia, Japan, Laos, Mozambique, Peru, Philippines, Somalia, Thailand, and Burma. Those who began pursuing BW in those years were South Africa, Libya, Cuba, Bulgaria, the USSR, Iran, Iraq, North Korea, Laos, and Vietnam. See tables 1 and 2 in Horowitz and Narang, "Poor Man's Atomic Bomb."

25 See also Horowitz and Narang, "Poor Man's Atomic Bomb." However, in practice, neither weapon really substitutes for a nuclear weapon. Chemical weapons in particular are not likely to be a good deterrent against a country armed with nuclear weapons because most countries that can afford nuclear weapons can also afford to give their militaries and citizens gas masks. Actually, chemical weapons are most effective against poor countries with large, compact populations, and underequipped troops (e.g., Iran in the 1980s). This point is made by Matthew Meselson, "Implications of the Kuwaiti Crisis for Chemical Weapons Proliferation and Arms Control," *Chemical Weapons and Security in the Middle East: Proceedings from a Congressional Briefing*, ed. Eric H. Arnett, American Association for the Advancement of Science Program on Science and International Security, Washington, DC, 1990, p. 16.

26 In 2002, videotapes emerged that showed al-Qaeda had successfully developed and tested cyanide and sarin. Nic Robertson, "Tapes Shed New Light on Bin Laden's Network," *CNN*, August 19, 2002, http://www.cnn.com/2002/US/08/18/terror.tape.

main/. In 1984, a religious cult called the Rajneeshee contaminated the salad bars in one Oregon county with salmonella. The plot led to 751 people becoming ill, but no one died. The second instance of BW was in 2001, when anthrax was sent in the mail on several occasions, but here as well, there were only 18-22 infected and five deaths. Ely Karmon, "Are the Palestinians Considering Biological Weapons?" ICT website, August 14, 2001, http://www.ict.org.il/articles/articledet.cfm?articleid=376. On the 2001 anthrax attacks, see "FBI Renews Search in Anthrax Probe," *CBS News.com*, December 12, 2002, http://www.cbsnews.com/stories/2002/09/04/national/main520719.shtml.

27 Karmon, "Are the Palestinians Considering Biological Weapons." However, recently, biological and chemical sciences have developed considerably. As a result, actors can now develop and manufacture more toxic, durable, and deadlier agents than ever before, at the same time that production has become both simpler and cheaper. In biology, the genetic engineering revolution, biotechnology, and "synthetic biology" allow the production of deadlier micro-organisms with relatively little expense and simple means. This development is a major challenge in defending against and preventing the proliferation of chemical and biological weapons.

28 President Richard Nixon, "Statement on Chemical and Biological Defense Policies and Programs," November 25, 1969, http://en.wikipedia.org/wiki/Statement_on_Chemical_and_Biological_Defense_Policies_and_Programs; Judith Miller, Stephen Engelberg, and William Broad, *Germs: Biological Weapons and America's Secret War*. (New York: Simon & Schuster, 2001). See also interview with Jeanne Guillemin.

29 Miller, Engelberg, and Broad, *Germs*; Phillip M. McCauley and Rodger A. Payne, "The Illogic of the Biological Weapons Taboo," *Strategic Studies Quarterly* 4 (2010): 6-35; and Tom Mangold, *Plague Wars: The Terrifying Reality of Biological Warfare* (New York: Macmillan, 1999).

30 For these reasons, the United States has led the opposition to a verification regime. Countries critical of America's stance claim that it is motivated mainly out of fear that verification would expose its supposed clandestine biological warfare activity which contradicts the BTWC. Despite the US objection to the verification regime, it is very supportive of the BTWC, arguing that the best way to implement the treaty is by prompting internal legislation in the member states, and by promoting and implementing defense and disease prevention. This is to be done by developing health and medicine systems, promoting interstate cooperation, and assisting developing countries – steps already taken by the United States. See, for instance, President Obama's National Strategy for Countering Biological Threats published in December 2009, http://www.whitehouse.gov/sites/default/files/National_Strategy_for_Countering_BioThreats.pdf.

31 Daniel Feakes, Brian Rappert, and Caitríona McLeish, "Introduction: A Web of Prevention?" in *A Web of Prevention: Biological Weapons, Life Sciences and the Governance of Research*, eds. B. Rappert and C. McLeish (London: Earthscan, 2007), p. 6, https://ore.exeter.ac.uk/repository/bitstream/handle/10036/31457/9781844073733.pdf?sequence=1.

32 As of January 2014, according to the website of the Organisation for the Prohibition of Chemical Weapons: http://www.opcw.org/about-opcw/member-states and http://www.opcw.org/about-opcw/non-member-states.

33 Brown (forthcoming) attempts to estimate this using W-NOMINATE, leveraging state signing decisions on other treaties, along with signing decisions of other states on the treaty in question, plus data on compliance for all states to estimate how much signing either document actually impacted on state behavior.
34 Based on data by Horowitz and Narang, "Poor Man's Atomic Bomb."
35 We believe the overwhelming importance of this factor is consistently underestimated by experts. For instance, Louise Arimatsu has written in "A Treaty for Governing Cyber-Weapons": "At its most basic, the different approaches pursued [by the US and Russia] are primarily, although not exclusively, a reflection of the different ideological viewpoints on the role of the State. A supplementary reason driving Russia's ambitions for an international cyber arms control treaty (and one that must not be under-estimated) is its perceived inferiority in field of communications technology," p. 5. Our point is that Russia's inferiority is not a supplementary reason for its leading the charge on a cyber convention while America drags its feet – it is *the* reason.
36 When one considers the difficulties the IAEA has had convincing countries about the nefarious programs of countries like Iran about its nuclear program – a relatively straightforward and clear program – then it is impossible to imagine an effective inspection regime convincing other countries that a cyber program was violating an agreement.
37 Rauscher and Korotkov, "Working towards Rules for Governing Cyber Conflict," p. 8.
38 Henry Maine, "Lecture VII: The Mitigation of War," Lectures on International Law, Project Avalon, http://avalon.law.yale.edu/19th_century/int07.asp. Richard Price, in contrast, argues that there is nothing inherent about the weapons themselves that led to the ban of these weapons, as opposed to the use of, for instance, flame throwers. Richard M. Price, *The Chemical Weapons Taboo* (Ithaca: Cornell University Press, 1997).