

Cyber Weapons Convention

Kenneth Geers

Naval Criminal Investigative Service (NCIS), Cooperative Cyber Defence Centre of Excellence (CCD COE) Tallinn, Estonia

ABSTRACT

World leaders are beginning to look beyond temporary fixes to the challenge of securing the Internet. One possible solution may be an international arms control treaty for cyberspace. The 1997 Chemical Weapons Convention (CWC) provides national security planners with a useful model. CWC has been ratified by 98% of the world's governments, and encompasses 95% of the world's population. It compels signatories not to produce or to use chemical weapons (CW), and they must destroy existing CW stockpiles. As a means and method of war, CW have now almost completely lost their legitimacy. This article examines the aspects of CWC that could help to contain conflict in cyberspace. It also explores the characteristics of cyber warfare that seem to defy traditional threat mitigation.

Keywords

Cyber attack, defense, arms control, Chemical Weapons Convention, CWC, Cyber Weapons Convention, Internet Security Convention

1. Introduction

The world has grown so dependent on the Internet that governments may seek far-reaching strategic solutions to help ensure its security. Every day, more aspects of modern society, business, government, and critical infrastructure are computerized and connected to the Internet. As a consequence and for the sake of everything from the production of electricity to the integrity of national elections, network security is no longer a luxury, but a necessity.

A fundamental challenge to better network security is that computers are highly complex objects that are inherently difficult to secure. The Common Vulnerabilities and Exposures (CVE) List grows by nearly a hundred every month.¹ There are likely more pathways into your computer network than your system administrators can protect. And to a large degree, this explains the high return on investment enjoyed by cyber criminals and cyber spies.

In the future, if war breaks out between two or more major world powers, one of the first victims could be the Internet itself. The reason is that classified cyber attack tools and techniques available to military and intelligence agencies are likely far more powerful than those available to the general public.² However, as with chemical weapons (CW) and even with nuclear weapons, it is

¹ "Common Vulnerabilities and Exposures List," The MITRE Corporation, <http://cve.mitre.org/>.

² Mike McConnell, former director of the U.S. National Security Agency and Director of National Intelligence recently wrote in the *Washington Post* that "the lion's share of cybersecurity expertise lies in the federal government" (McConnell, 2010).

possible that non-state actors including terrorists will acquire strategically significant cyber attack tools and techniques in the future.³

What is to be done? Severing one's connection to cyberspace is not an attractive option. The benefits of connecting to the Internet usually outweigh the drawbacks; this quickly undermines a fortress mentality. And even theoretically "closed" networks – those with no direct connection to the Internet – are still subject to a wide range of computer network attacks (CNA).⁴

In light of our dependence on such vulnerable technology, and due to the fact that CNA is difficult to stop, world leaders may try to negotiate international agreements designed to contain conflict on the Internet.⁵ Cyber arms control is one possible strategy, and the 1997 Chemical Weapons Convention (CWC) may provide a strong candidate model.⁶

2. Chemical Weapons Convention

Chemical weapons (CW) are almost as old as warfare itself. Archeologists have found poison-covered arrowheads dating to 10,000 BC (Mayor, 2008). In the First World War, CW may have caused one-third of the estimated 5 million casualties. Today, terrorists are attracted to CW not only for its killing power but also due to its ease of acquisition (Newmark, 2001).

As a weapon, CW employs the toxic properties of certain chemicals in a way that can kill, injure or incapacitate humans and animals. Throughout history, each new generation of CW has been more dangerous than its predecessor (*Ibid*).

In 1997, 95 nations signed CWC, an international arms control agreement that has been a success by almost any measure. The treaty's purpose is reflected in its full name: *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction*. Its goal is to eliminate the entire category of weapons of mass destruction (WMD) that is associated with toxic chemicals and their precursors. The CWC Preamble declares that achievements in chemistry should be used exclusively for beneficial purposes, and that the prohibition on CW is intended "for the sake of all mankind."

Each signatory is responsible for enforcing CWC within its legal jurisdiction. This includes overseeing the destruction of existing CW and the destruction of all CW production facilities. Under the convention, all toxic chemicals are considered weapons unless they are used for purposes that are specifically authorized under CWC. Further, members are prohibited from transferring CW to or from other nations.

³ James Lewis of CSIS recently stated: "It remains intriguing and suggestive that [terrorists] have not launched a cyber attack. This may reflect a lack of capability, a decision that cyber weapons do not produce the violent results terrorists crave, or a preoccupation with other activities. Eventually terrorists will use cyber attacks, as they become easier to launch..." (Lewis, 2010).

⁴ Military and intelligence agencies are capable of supply chain attacks, insider exploitation, the standoff kinetic destruction of computer hardware, and the use of electromagnetic radiation to destroy unshielded electronics via current or voltage surges.

⁵ According to *The New York Times*, Russian negotiators have long argued that an international treaty, similar to those that have been signed for WMD, could help to mitigate the threat posed by military activities to civilian networks, and that in 2009 the U.S. appeared more willing to discuss this strategy (Markoff & Kramer, 2009).

⁶ Others could be the Nuclear Non-Proliferation Treaty or the Biological Weapons Convention.

CWC is administered by the Organisation for the Prohibition of Chemical Weapons (OPCW), based in The Hague, which is an independent entity that works in concert with the United Nations. OPCW has a staff of 500 and a budget of EUR 75 million.⁷

Currently, 188 nations, encompassing 98% of the global population, are party to CWC. A mere 13 years old, CWC has enjoyed the fastest rate of accession of any arms control treaty in history.⁸ Since 1997, over 56% of the world's declared stockpile of 71,194 metric tons of chemical agent has been destroyed, along with almost 50% of the world's 8.67 million chemical munitions and containers.⁹

3. CWC: lessons for cyber conflict

Governments addressed the threat from CW by creating CWC. In order to counter the threat posed by cyber attacks and cyber warfare, world leaders may decide to create a similar regime, a *Cyber Weapons Convention*. In that event, international negotiators will likely examine CWC to see whether its principles are transferrable to the cyber domain. This author has identified five principles characteristic of CWC that may be useful in this context: political will, universality, assistance, prohibition, and inspection.¹⁰

Political will. On March 21, 1997, Presidents Bill Clinton and Boris Yeltsin issued a joint statement from Helsinki, stating that they were committed to the ratification of CWC in order to “banish poison gas from the Earth” (UCSB, 2010). At the end of the Cold War, the U.S. and Russia possessed the lion's share of CW, and CWC could not have been a success without their leadership. However, all signatories must be convinced that they have more to gain from joining CWC than they have to lose by remaining outside it. In the case of CW, there is a genuine abhorrence that the science of chemistry has been used for such lethal purposes, as well as a fear that terrorist groups – who lack the accountability of sovereign governments – will obtain CW.

Universality. In 1997, more than two dozen countries possessed CW (Cole, 1996). Furthermore, CW technology was not difficult to acquire, so that number would have continued to grow. CWC authors therefore designed the convention as a universal treaty with a universal and permanent goal. All nations are encouraged to become members, and the treaty's endgame is the elimination of an entire class of WMD. CWC therefore represents the broadest possible multilateral security framework. At first glance, this strategy could be an obstacle to treaty advancement. However, universality also provides a strong recruitment incentive: peer pressure. A higher ratio of members to non-members increases one's sense of security gained by accession, and heightens the isolation felt by those who remain on the outside.

Assistance. OPCW offers enormous practical aid to CWC members. Above all, signatories are helped to fulfill treaty requirements, beginning with the destruction of CW and CW production facilities. Further, OPCW actively promotes the advancement of peaceful uses of chemistry for

⁷ OPCW website: www.opcw.org.

⁸ Challenges remain: Angola, Egypt, Israel, Myanmar, North Korea, Somalia, and Syria are still outside CWC; the U.S. and Russia must quicken their pace of CW destruction to meet the legally binding deadline of April 2012; advances in science and technology pose constant challenges to the integrity of the inspections regime.

⁹ OPCW website: www.opcw.org.

¹⁰ I derived these five principles in part from the article Mikhail Gorbachev and Rogelio Pfirter wrote for *Bulletin of the Atomic Scientists* and Oliver Meier's interview with Pfirter in *Arms Control Today*.

economic development. This includes the provision of training for local experts. Finally, OPCW offers advocacy to treaty members in the event they are threatened by the CW of another state.

Prohibition. CWC has proven that verifiable destruction of CW and their production facilities is feasible. By 2010, over 50% of the world's declared chemical agent stockpiles had been verifiably destroyed, as well as nearly 50% of declared chemical munitions. Some states had completely eliminated their CW programs. At the current rate, over 90% of the world's known CW will be destroyed by 2012. Although seven nations remain outside CWC, no new states have acquired CW since 1997. The success of CWC stands in contrast to the 1968 Nuclear Non-Proliferation Treaty (NPT). Despite the efforts of NPT, the size of the world's nuclear club has grown from five¹¹ to nine.¹²

Inspection. Since 1997, almost 4,000 CWC inspections have been conducted on the territory of 81 member states in order to verify treaty compliance. These have taken place at almost 200 known CW-related sites and at over 1,000 other industrial sites. Nearly 5,000 facilities around the world are liable to CWC inspection at any time. One of the primary benefits of CWC membership is the right to request a "challenge inspection" on the territory of a fellow member state, based on the principle of "anytime, anywhere," with no right of refusal.

4. Toward a Cyber Weapons Convention

Cyber warfare is not chemical warfare. Although they share some similarities – including ease of acquisition, asymmetric damage, and polymorphism – the tactics, strategies and effects are fundamentally different. Chemical warfare kills humans; cyber warfare kills machines.¹³

As a means of waging war, however, both chemical and cyber attacks represent a potential threat to national security. As such, diplomats may be asked to negotiate international agreements designed to mitigate the risk of cyber warfare, just as they have done for CW.

The five principles described in the previous section have helped to make CWC a success. In this section, the author argues that the first three principles are clearly transferable to the cyber domain, while the final two are not.

Political will. International treaties require widespread agreement on the nature of a common problem. The threat posed by cyber attacks – based on national capabilities as well as the fear that terrorists will begin to master the art of hacking – could be strong enough to form such a political consensus. In May 2009, President Obama made a dramatic announcement: "cyber attacks have plunged entire cities into darkness" (White House, 2009). Media reports state that the attacks took place in Brazil, affected millions of civilians in 2005 and 2007, and that the source of the attacks is still unknown (CBS, 2009). The more recent cyber attack on Google was serious enough to begin discussion in the U.S. on whether to create an ambassador-level post, modeled on the State Department's counterterrorism coordinator, to oversee international cyber security efforts (Gorman, 2010). As with CWC, a convention intended to help secure the Internet would need the major world

¹¹ These are also the permanent members of the United Nations Security Council: China, France, Russia, UK, and the U.S.

¹² De facto members now include India, Israel, Pakistan, and North Korea (Huntley, 2009).

¹³ To be more specific, cyber attacks usually target the data resident on or functionality of a machine. It is also important to note that inoperable machines can kill humans: examples include medical equipment and national air defense systems. By the same token, chemical warfare can also kill flora, fauna, and human input to machines.

powers behind it to succeed. At a minimum, in today's world that means the U.S., Russia, China, and the EU.¹⁴

Universality. One of the primary challenges to improved computer security is the fact that the Internet is a worldwide enterprise. The jurisdiction of law enforcement and counterintelligence personnel ends every time a network cable crosses an international border. Even though thousands of miles may separate an attacker and defender in the real world, everyone is a neighbor in cyberspace, and attackers often have direct access to their victims. Smart hackers hide within the maze-like architecture of the Internet, and route attacks through countries with which the victim's government has poor diplomatic relations or no law enforcement cooperation. In 2010, there are plenty of cyber safe havens where criminals, spies and terrorists can operate without fear of reprisal (Gray & Head, 2009). Although the global nature of cyberspace makes the practical task of securing the Internet inherently more difficult, the universal goals of CWC are highly appropriate in the cyber domain. Politicians, international negotiators, and the public will have no trouble understanding this characterization, and universality would be a cornerstone of a Cyber Weapons Convention.

Assistance. Vulnerabilities in computer networks and the advantages they create for an attacker will persist for the foreseeable future. Organizations have no choice but to invest more time and effort into computer security. However, a proper implementation of best practices such as risk management, awareness training, defense-in-depth and incident handling¹⁵ usually requires more expertise and resources than most organizations and even many countries have available. Within CWC, OPCW offers practical aid to its members; in the same fashion, a Cyber Weapons Convention could create an internationally-staffed institution dedicated to helping signatories improve their cyber defense posture, and respond effectively to cyber attacks when they occur. Experts could provide technical, legal, and policy advice via consultation and training. A crisis response team could be available to deploy worldwide at a moment's notice, ready to publish its findings to the world. And as with CWC, the institution could actively promote the benefits of peaceful uses of computer technology for economic development and cooperation.

One significant but difficult step for governments to take would be the joint instrumentation and observation of the Internet and its network traffic flows. Many cyber threats, such as that posed by botnet technology, simply move too quickly for the kind of traditional inspections that OPCW provides. Cyber attack mitigation requires immediate source identification and the ability to cross technical, legal, and national borders quickly. The best chance that future Cyber Weapons Convention monitors would have is with access to real-time network data from across the whole of the Internet, and the ability to collaborate immediately with treaty-empowered colleagues throughout the world.¹⁶ National sovereignty and data privacy concerns would have to be carefully guarded. The technical and forensic side of the regime should be separated as much as possible from its legal and political ramifications. Data analysts could not have access to any personally identifiable information, but when cyber attacks are observed, the appropriate law enforcement organizations must be notified.

¹⁴ With CWC, the Middle East conflict continues to pose the most serious challenge to worldwide agreement, and it could do the same for a Cyber Weapons Convention.

¹⁵ For example, the U.S. Computer Emergency Readiness Team (US-CERT) offers many free publications in the following categories: "General Internet security," "Securing your computer," "Recovering from an attack," and "Monthly and quarterly reports" (www.us-cert.gov/reading_room/); however, most system administrators simply do not have the time to study, absorb, and implement all such recommendations.

¹⁶ Such an effort would be daunting from a technical perspective, but in theory, if this is possible to accomplish in one large country, it should be possible across the globe. On a human level, thousands of international CERT personnel already do it on a less formal basis every day.

Prohibition. The proof that CWC has been a success lies in the large volume of CW that has been verifiably destroyed. The principle of prohibition, however, would be the most challenging aspect of CWC to apply in cyberspace. Malicious computer code is notoriously difficult to define. In the single month of May 2009, Kaspersky Anti-Virus Lab found 42,520 “unique malicious, advertising, and potentially unwanted” programs on its clients’ computers (Kaspersky, 2009). Even in a well-designed and malware-free network, a legitimate path for remote system administration can be used by a masquerading hacker, who has correctly guessed or stolen its password, to thoroughly undermine its confidentiality, integrity, and/or availability. Any computer programmer can learn to write malware, and non-programmers can simply download professional-quality attack tools from well-known websites. Further, cyber warfare is unlike chemical warfare in that cyber attacks often demand stealth and anonymity. At a minimum, any prohibition on malware will require substantial progress on solving the cyber attack “attribution” problem.¹⁷ This will take time, and involve technical, legal, and international cooperation on a level far higher than it exists today.

Inspection. Similar to prohibition, the CWC inspection regime has been a success, but it is difficult to imagine how the principle of inspection could easily be applied in cyberspace. Around the world, 5,000 industrial facilities are subject to CWC inspection at any time; this is a large but manageable number. Compare it to the amount of digital information that can be placed on one removable thumb drive. In 2010, a 256 GB USB Flash drive costs under \$1000;¹⁸ it holds over 2 trillion bits of data. Even widely-published operating system and application code can be almost impossible to understand thoroughly – even for experts – as there is simply too much information to analyze (Cole, 2002).¹⁹ Malware can be written on any computer, and transmitted to the Net from any network access point. In the U.S. alone, there are 383 million computers connected directly to the Internet.²⁰ In theory, a Cyber Weapons Convention could require closer inspection and monitoring at the Internet Service Provider (ISP) level. However, such regimes are already commonplace, such as China’s Golden Shield Project, the European Convention on Cybercrime, Russia’s SORM,²¹ and the USA PATRIOT Act. Each is unique in terms of guidelines and enforcement, but all face the same problem of overwhelming traffic volume.

5. Conclusion

The challenge of securing the Internet appears to be worsening with time (Geers, 2010). World leaders may eventually decide that the best way to mitigate the threat posed by cyber attacks is by signing an international cyber arms control treaty.²²

¹⁷ This refers to anonymous cyber attacks, described in the Universality section above.

¹⁸ The Kingston DataTraveler® 310 is currently advertised as the highest capacity USB Flash drive on the market.

¹⁹ Even if it were possible, software is dynamic. Programs constantly change their functionality via security patches and other updates.

²⁰ This figure is from *The World Factbook*, published by the U.S. Central Intelligence Agency, and describes the number of “Internet hosts” in a country. These are defined as “a computer connected directly to the Internet ... Internet users may use either a hard-wired terminal ... or may connect remotely by way of a modem via telephone line, cable, or satellite to the Internet Service Provider’s host computer.”

²¹ Система Оперативно-Розыскных Мероприятий or “System for Operative Investigative Activities.”

²² Many vignettes could be recited here. In 2007, German Chancellor Angela Merkel visited China for a state meeting that was overshadowed by a media claim that Chinese hackers had been caught attempting to steal data from Merkel’s chancellery and other Berlin ministries. The Chinese government denied the allegations, but Prime Minister Wen Jiabao nonetheless told Merkel that measures would be taken to “rule out hacking attacks”

The Chemical Weapons Convention (CWC) constitutes a useful model. It boasts the vast majority of world governments as signatories and has tangibly reduced the threat of chemical warfare, both by delegitimizing the use of chemical weapons (CW) and by dramatically reducing the quantity of CW in existence.

This article highlights five principles that have helped to make CWC a success, and examines each principle to see whether it could support the development of a *Cyber Weapons Convention*.

The first three principles – political will, universality, and assistance – are easy to apply in the cyber domain. None of them is a perfect fit, but as with CWC, all of them are appropriate to the nature and challenges of managing Internet security.

The final two principles – prohibition and inspection – are not helpful at this time. It is difficult to prohibit something that is hard to define, and not easy to inspect something that grows by orders of magnitude on a regular basis. In fact, these two catches could prove significant enough that a future treaty may not be called *Cyber Weapons Convention*, but something more generic such as *Internet Security Convention*.

On balance, the three applicable principles provide world leaders with a good starting point to explore the prospects for a *Cyber Weapons Convention*. If national and Internet security thinkers decide that an international cyber arms control treaty is the right way forward, political leaders may give scientists the funding they need to attack the technical challenges of prohibition and inspection.

Kenneth Geers (kenneth.geers@ccdcoe.org) *Naval Criminal Investigative Service (NCIS) Cooperative Cyber Defence Centre of Excellence (CCD COE)*

References

- Cody, E. (2007, Sep 13). "Chinese Official Accuses Nations of Hacking." *Washington Post*.
- Cole, L. A. (1996). "Countering Chem-Bio Terrorism: Limited Possibilities." *Politics and the Life Sciences*. 15(2), 196.
- "Cyber War: Sabotaging the System." (2009, Nov 8). *60 Minutes: CBS*.
- "Espionage Report: Merkel's China Visit Marred by Hacking Allegations." (2007, Aug 27). *Spiegel*.
- Geers, K. (2010, Spring). "A Brief Introduction to Cyber Warfare." *Common Defense Quarterly*.
- Gorbachev, M. & Pfirter, R. (2009, Jun 16). "Disarmament lessons from the Chemical Weapons Convention." *Bulletin of the Atomic Scientists* online.
- Gorman, S. (2010, Mar 23). "U.S. Aims to Bolster Overseas Fight Against Cybercrime." *The Wall Street Journal*.
- Gray, D.H. and Head, A. (2009). "The importance of the internet to the post-modern terrorist and its role as a form of safe haven." *European Journal of Scientific Research*, 25(3), 396-404.
- Huntley, W. L. (2009). "Abandoning Disarmament? The New Nuclear Nonproliferation Paradigms." In D. Krieger (Ed.) *The Challenge of Abolishing Nuclear Weapons*. New Jersey: Transaction Publishers.
- Lewis, J.A. (2010). "The Cyber War Has Not Begun." *Center for Strategic and International Studies*.

(*Spiegel*, 2007). The following month, Chinese Vice Information Industry Minister Lou Qinqian wrote in a Communist Party magazine that foreign intelligence services had also caused "massive and shocking" damage to China via computer hacking (Cody, 2007).

- Markoff, J. & Kramer, A. (2009, Dec 13). "In Shift, U.S. Talks to Russia on Internet Security." *The New York Times*.
- Mayor, A. (2008). *Greek Fire, Poison Arrows, and Scorpion Bombs: Biological & Chemical Warfare in the Ancient World*, Overlook TP.
- McConnell, M. (2010, Feb 28). "Mike McConnell on how to win the cyber-war we're losing." *Washington Post*.
- Meier, O. (2007). "The Chemical Weapons Convention at 10: An Interview with OPCW Director-General Rogelio Pflirter." *Arms Control Today*. 37(3), 14.
- "Monthly Malware Statistics: May 2009." Kaspersky Lab website: www.kaspersky.com.
- Newmark, J. (2001). "Chemical warfare agents: A primer." *Military Medicine*. 166(12), 9.
- "The President's News Conference with President Boris Yeltsin of Russia in Helsinki." (1997). *The American Presidency Project*, UC Santa Barbara.
- "Remarks by the President on Securing our Nation's Cyber Infrastructure." (2009). *The White House: Office of the Press Secretary*.