

2015

21st Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and WMDs

Mary Ellen O'Connell

Notre Dame Law School, maryellenoconnell@nd.edu

Follow this and additional works at: http://scholarship.law.nd.edu/law_faculty_scholarship

 Part of the [Military, War, and Peace Commons](#), [Science and Technology Law Commons](#), and the [Second Amendment Commons](#)

Recommended Citation

O'Connell, Mary Ellen, "21st Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and WMDs" (2015). *Journal Articles*. 1144.

http://scholarship.law.nd.edu/law_faculty_scholarship/1144

This Article is brought to you for free and open access by the Publications at NDLScholarship. It has been accepted for inclusion in Journal Articles by an authorized administrator of NDLScholarship. For more information, please contact lawdr@nd.edu.

Washington University Global Studies Law Review

Volume 13


Issue 3 *The Legal Challenges of Globalization: A View from the Heartland (Symposium Edition)*

2014

21st Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and WMDs

Mary Ellen O'Connell

Follow this and additional works at: http://openscholarship.wustl.edu/law_globalstudies

 Part of the [Ethics and Professional Responsibility Commons](#), [Human Rights Law Commons](#), [International Law Commons](#), [Military, War and Peace Commons](#), [National Security Commons](#), [Politics Commons](#), and the [Science and Technology Commons](#)

Recommended Citation

Mary Ellen O'Connell, *21st Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and WMDs*, 13 WASH. U. GLOBAL STUD. L. REV. 515 (2014),
http://openscholarship.wustl.edu/law_globalstudies/vol13/iss3/11

This Article is brought to you for free and open access by the Law School at Washington University Open Scholarship. It has been accepted for inclusion in Washington University Global Studies Law Review by an authorized administrator of Washington University Open Scholarship. For more information, please contact emily.stenberg@wustl.edu, digital@wumail.wustl.edu.

21ST CENTURY ARMS CONTROL CHALLENGES: DRONES, CYBER WEAPONS, KILLER ROBOTS, AND WMDS

MARY ELLEN O'CONNELL*

Dean David Wippman's remarks at the 2013 Midwest Meeting of the International Law Association focused on how we in international law struggle with the view that international law is not really law—or not really law when it comes to the use of military force. Students of legal theory will tell you, however, that defining law poses challenges in all areas of law. Understanding what counts as law is no simple task. Still, the question of whether international law is really law may be more important, especially when it comes to the use of force, because the stakes are so high. Indeed, the stakes are probably higher than with respect to any other body of rules.

Compare, for example, the city of Chicago where the law against murder is frequently violated. In 2012, 500 people were murdered in Chicago;¹ few of the perpetrators will ever be identified, let alone prosecuted. When the rules on the use of force are violated, it is not hundreds that will die but hundreds of thousands. We typically know who is ultimately responsible for the resort to unlawful war and the resulting loss of life and destruction, but rarely are such persons prosecuted. In both contexts—domestic law against murder and international law against war—we must do better. I choose to work in the area of law against war and accept the challenge of persuading others as to why the law of the United Nations Charter binds the United States and all states, and why it matters that the United States and all states comply with this law. The task is challenging for a number of reasons, including the apparent decline in general knowledge respecting international law in the United States and the popularity of resort to military force. During 2013, however, we could see several indications that Americans were thinking differently about war. “War fatigue” has become a common phrase. The poor results and unintended consequences of major wars involving the United States

* Robert and Marion Short Professor of Law and Research Professor of International Dispute Resolution, Kroc Institute for International Peace Studies, University of Notre Dame; with thanks for excellent research assistance to Sean Parish (JD expected 2015).

1. U.S. DEP'T OF JUSTICE, FED. BUREAU OF INVESTIGATION, CRIM. JUST. INFO. SERVICES DIVISION, *Crime in the United States: Illinois*, FBI.GOV, http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-2012/tables/8tabledatadecpdf/table-8-state-cuts/table_8_offenses_known_to_law_enforcement_by_illinois_by_city_2012.xls (last updated June 13, 2013).

against Serbia (1999), Afghanistan (2001–), Iraq (2003–), and Libya (2011–) are apparent.

Moreover, rather than resort to armed force in Syria in August 2013 over the use of chemical weapons, diplomacy prevailed and an agreement backed by a UN Security Council resolution led quickly to progress in the demolition of Syria's chemical weapons capacity.² If Syrian chemical weapons are destroyed through the art of diplomacy, we may see a revival of interest in alternatives to military force even in Washington, D.C. In September 2013, President Obama spoke by telephone with Iran's President Rouhani, giving further support to the view that diplomacy might be on an upswing.³

If the United States is moving toward a less militaristic phase, it will be an important time for international law specialists. We need to be ready to fill the knowledge vacuum when asked how the United States can forgo military force and yet promote security, prosperity, human dignity, and the natural environment both in the United States and in the world. Too many Americans—on the left and the right—have believed for too long that military force is the most effective way to deal with a range of complex problems from human rights violations to terrorism to arms control. The focus of these remarks is on the last problem in the list: arms control.⁴ International law clearly prohibits the use of military force for arms control, but that is not the end of the story. International law embraces alternatives to the use of force to control certain weapons and certain weapons systems. I will illustrate this contrast of lawful and unlawful means by looking at four weapons categories:

- WMDs, or weapons of mass destruction, which are chemical, biological, and nuclear weapons;
- Drones, or unmanned aerial launch vehicles; the United States also possesses unmanned land and sea launch vehicles;
- Cyber weapons, which are computer programs designed to have destructive capacity; and the newest category,

2. See S.C. Res. 2118, U.N. Doc. S/RES/2118 (Sept. 27, 2013).

3. See *Iran News Round Up*, IRAN TRACKER (Apr. 10, 2013), <http://www.irantracker.org/iran-news-round-april-10-2013>.

4. For a general introduction to the international law restricting resort to force, see Mary Ellen O'Connell, *The Prohibition of the Use of Force*, in RESEARCH HANDBOOK ON CONFLICT AND SECURITY LAW: JUS AD BELLUM, JUS IN BELLO, JUS POST BELLUM 89 (Nigel White & Christian Henderson eds., 2013).

- Fully autonomous weapons systems, which are robotic weapons programed to select and attack targets without further human intervention following the initial programing of the robot.⁵

All four categories pose challenges for the international community. Although chemical, biological, and nuclear weapons are clearly unlawful to use, a few states still possess them and, in the case of nuclear weapons, may even be seeking to obtain them.⁶ Respecting unmanned, cyber, and fully autonomous weapons, certain commentators in the international security field indicate they are unaware of relevant international legal rules or seem to believe international law should play no role in regulating their use.⁷

International law does exist respecting all of these weapons categories. Moreover, looking to the lessons taught by twentieth century arms control efforts, we find that international law is uniquely effective and appropriate for regulating weapons. Here are just three constructive lessons from twentieth century arms control:

1. Controlling weapons proliferation by trying to keep a monopoly on technology or by staying ahead in technological development has not worked.
2. Attempting to control weapons development, proliferation, or use through unlawful means, such as the use of force, has proven ineffective and counter-productive.
3. Using the lawful means available in international law has succeeded in controlling weapons and in achieving other desiderata of the international community.

We will begin by looking first at nuclear weapons, then at the other weapons categories.

NUCLEAR WEAPONS

Most will know at least the outlines of the story of the secret Manhattan project to produce an atomic bomb during World War II.

5. See Rob Sparrow, *Killer Robots*, 24 J. APPLIED PHIL. 62 (2007).

6. This is the conclusion of some respecting Iran, despite Iran's official position that it is developing a domestic nuclear power capacity, not nuclear weapons.

7. See, e.g., the comments of a former National Security Agency lawyer, Stewart Baker, *Denial of Service, Lawyers are Crippling America's Ability to Defend Against Cyberwar with Arcane Rules and Regulations*, FOREIGN POL'Y (Sept. 30, 2011), http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service.

Thanks in large part to old-fashioned espionage, the Soviets quickly acquired the technology to create their own atomic weapons. As Robert O'Connell describes in his book *Of Arms and Men*:

Initially, Americans dealt with the bomb from the perspective of their own enormous postwar national power and the presumption of a nuclear monopoly of some considerable duration [Then] on 3 September 1949 a B-29 flying over the South Pacific detected higher than normal radiation levels explicable only in terms of a Russian atomic bomb test. After only four short years, the nuclear monopoly had ended.⁸

Since 1949, both lawful and unlawful measures have been taken to try to prevent more states from acquiring nuclear weapons. Starting with several examples of unlawful measures, we will quickly see that such measures have been inadequate and even counter-productive. In 1981, Israeli jets bombed a nuclear reactor under construction at Osirik, Iraq. The Security Council unanimously condemned the bombing as a violation of United Nations Charter Article 2(4) that was not excused as an exercise of self-defense under Article 51 of the Charter.⁹ In the Security Council debate, most delegations pointed to the absence of an armed attack by Iraq on Israel as the most important missing element for lawful self-defense. States made it clear that they do not equate a future risk of nuclear attack with the armed attack requirement of Article 51.

The American representative to the UN Security Council, Ambassador Jeanne Kirkpatrick, stated that the United States, too, understood Israel had violated the Charter, in particular because Israeli leaders had not exhausted peaceful alternatives before ordering the attack. Many representatives were impressed by the testimony of the Director General of the International Atomic Energy Agency that the IAEA had found no evidence of unlawful weapons development by the Iraqi government, such as diversion of nuclear material. Following Israel's attack, Iraq did pursue nuclear weapons, but did so secretly in protected sites.¹⁰ Following the 1991 Gulf War, the United Nations undertook concerted steps to ensure the elimination of all WMDs in Iraq. Those efforts succeeded well before the United States, United Kingdom, and Australia invaded in 2003. In

8. ROBERT L. O'CONNELL, *OF ARMS AND MEN, A HISTORY OF WAR, WEAPONS, AND AGGRESSION* 303 (1989).

9. See S.C. Res. 487, U.N. Doc. S/RES/487 (June 19, 1981), and accompanying debate.

10. *Country Profiles: Iraq*, NUCLEAR THREAT INITIATIVE, <http://www.nti.org/country-profiles/iraq> (last visited Jan. 23, 2014).

letters to the Security Council, the three invading states sought to justify their resort to force as enforcement of Security Council resolutions mandating that Iraq eliminate its WMD programs.¹¹

Israel has also sought to prevent Iran from acquiring nuclear weapons through a variety of means, including assassinations of scientists.¹² The United States has denied any involvement in violent action within Iran; Israel refuses to comment.¹³ Nevertheless, the United States has said that military force against Iran is “on the table.”¹⁴ Whether Iran’s nuclear ambitions have been slowed by either tactic is difficult to say. Some Iranian hardliners have likely cited the threats of military force to support the acquisition of nuclear weapons and to do so as soon as possible. Most observers credit tough economic sanctions as providing the pressure necessary to bring about the new round of negotiations with Iran that began in 2013.¹⁵

Another unlawful measure taken against Iran has been the Stuxnet worm, apparently released by one or more governments, most likely the United States and Israel, in 2009–10 to slow the progress of Iran’s nuclear program.¹⁶ Stuxnet attacked computers manufactured by Siemens and used in the Iranian nuclear program. The effect of the worm in Iran was to cause centrifuges to turn far more rapidly than appropriate. In early 2011, officials in Israel and the United States announced that Iran’s nuclear program had been set back “by several years.” The Stuxnet worm, however, affected computers in other countries as well, including India, Indonesia, and Russia. Indeed, it is believed that forty percent of the computers affected were outside Iran. Stuxnet is said to be “the first-

11. Letter of John Negroponte, former United States Ambassador to the United Nations, to the President of the Security Council (Mar. 20, 2003) (on file with author).

12. Saeed Kamali Dehghan, *Iran Nuclear Scientist Killed in Tehran Motorbike Bomb Attack*, GUARDIAN (Jan. 11, 2012), <http://www.theguardian.com/world/2012/jan/11/iran-nuclear-scientist-killed>.

13. See Thomas Erdbrink & Joby Warbrick, *Iranian Scientist Involved in Nuclear Program Killed in Tehran Bomb Attack*, WASH. POST (Jan. 11, 2012), http://www.washingtonpost.com/world/iranian-scientist-killed-in-tehran-bomb-attack/2012/01/11/gIQAT1V7pP_story.html.

14. Mark Landler, *Obama Says Iran Strike Is an Option, but Warns Israel*, N.Y. TIMES (Mar. 2, 2012), http://www.nytimes.com/2012/03/03/world/middleeast/obama-says-military-option-on-iran-not-a-bluff.html?pagewanted=all&_r=0.

15. This is the position taken by President Obama. See *Deal Reached on Implementing Iranian Nuclear Agreement*, AL JAZEERA AMERICA (Jan. 12, 2013), <http://america.aljazeera.com/articles/2014/1/12/report-iran-saysallsidesagreeonucleardeal.html>.

16. James Hilder, *Computer Virus Used to Sabotage Iran’s Nuclear Plan “Built by US and Israel”*, AUSTRALIAN (Jan. 27, 2011), <http://www.theaustralian.com.au/news/world/>.

known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.”¹⁷

Ralph Langner, a German computer security expert, is convinced Stuxnet is a government-produced worm: “This is not some hacker sitting in the basement of his parents’ house. To me, it seems that the resources needed to stage this attack point to a nation state.”¹⁸ In another interview, Langer added: “Code analysis makes it clear that Stuxnet is not about sending a message or providing a concept. It is about destroying its targets with utmost determination in military style . . .”¹⁹ The worm may have slowed Iranian progress for some months, but it is now in the hands of criminal hackers and governments everywhere.

In short, the use of military force, assassinations, threats of force, and cyber attacks have all proven ineffective to end nuclear programs. By contrast to these various unlawful means, lawful means available within international law have proven successful without serious negative and unintended consequences. Thanks to the Treaty on Non-Proliferation of Nuclear Weapons (NPT),²⁰ the vast majority of states in the world do not possess nuclear weapons and do not seek them. This is an extraordinary accomplishment. Of the 193 sovereign states in the world that are members of the United Nations, only nine have nuclear weapons and only one state, Iran, is allegedly seeking them.

Through the NPT, an international legal instrument, the world has built an important norm against the possession or use of nuclear weapons. Moreover, the weight of evidence indicates that with a greater effort by the United States, the newer nuclear powers—India, Israel, North Korea, and Pakistan—might not have acquired nuclear weapons or might have been persuaded to give them up by now. Libya and Brazil were both persuaded to give up nuclear weapons programs. South Africa and Ukraine were persuaded to actually give up the weapons they possessed. Iraq gave up its nuclear ambitions following its defeat in the Gulf War of 1991. UN weapons inspectors succeeded in exposing Iraq’s program, and it was dismantled. Then thanks to the sanctions imposed on Iraq, which were enforced by NATO and largely by the United States, Iraq was never able to acquire inputs to any of its WMD programs. The human rights advocacy community heavily criticized the sanctions regime and even

17. Johnathan Fildes, *Stuxnet Work “Targeted High-Value Iranian Assets”*, BBC (Sept. 23, 2010), <http://www.bbc.co.uk/news/technology-11388018>.

18. *Id.*

19. Hilder, *supra* note 16.

20. July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S. 161.

those who defended it.²¹ Yet the defenders could tell the sanctions were working to prevent Saddam Hussein from building WMDs. The UN's Oil for Food program assured Iraq's ability to purchase food and medicine for the population. It was Saddam's decision to warehouse the purchases to create a media impression of the devastating impact of sanctions. In fact, Saddam Hussein had no WMDs by 2003, but did have warehouses full of food and medicine.

At the urging of the Soviet Union, North Korea joined the NPT in December 1985. In 1994, the U.S. was able to persuade North Korea to suspend building its own nuclear power capacity in exchange for two light water reactors.²² The Clinton administration never delivered the reactors. North Korea subsequently withdrew from the NPT in 2003 and began developing a nuclear weapons capacity.²³ The Bush administration made a new pledge to supply the reactors in 2005. It, too, failed to fulfill the U.S. promise. By 2006, North Korea had a nuclear weapon.²⁴ No one can say with certainty whether North Korea would have lived up to its end of the bargain, but under international law, North Korea's performance of its promise was premised on the prior U.S. performance.

Iran, the IAEA, which monitors the NPT, the United States, UK, Germany, France, China, and Russia are at the time of this writing involved in intense negotiations to end the conflict over Iran's nuclear program. Iran's President, Hassan Rouhani, invited new negotiations on Iran's nuclear problem soon after the U.S. turn to diplomacy respecting Syrian chemical weapons, a turn that included a move away from a military attack.²⁵ Successful negotiations will require following the classic steps of *Getting to Yes*.²⁶ Both sides will need to consider what the other needs in order to agree to concessions.

21. One of the most critical assessments of sanctions on Iraq used a title that entered the vernacular: "Sanctions of Mass Destruction." John Mueller & Karl Mueller, *Sanctions of Mass Destruction*, 78 FOREIGN AFF. 43 (1999).

22. *The U.S.-North Korean Agreed Framework at a Glance*, ARMS CONTROL ASSOC. (Aug. 2004), <http://www.armscontrol.org/factsheets/agreedframework>.

23. *Id.*

24. Erik Mobernd, *The Road to North Korea's Nuclear Test*, WORLD SECURITY NETWORK (Oct. 8, 2006), <http://www.worldsecuritynetwork.com/Koreas/erik-mobernd/The-Road-to-North-Korea%E2%80%99s-Nuclear-Test>.

25. See Symposium, *The U.S.-Iranian Relationship and the Future of International Order*, 2 PENN. ST. J.L. & INT'L AFF. 237 (2013), available at <http://elibrary.law.psu.edu/jlia/vol2/iss2/12/>.

26. ROGER FISHER & WILLIAM URY, *GETTING TO YES: NEGOTIATING AGREEMENT WITHOUT GIVING IN* (1983).

UNMANNED WEAPONS

Arguably, the first major revolution in military weapons development since the advent of nuclear weapons is owed to the computer. Computers have revolutionized war fighting in many ways, but computer-controlled unmanned launch vehicles are the weapons part of the revolution. The United States developed a drone at the end of World War II or soon after. Drones were used for reconnaissance in Vietnam, the Gulf War, the Balkans conflicts, and in all wars since. The first use of a drone in a lethal operation occurred in November, 2001 in the Afghanistan War. The legality of that use is hard to dispute, given that the United States was engaged in armed conflict with the Taliban and al Qaeda in Afghanistan at the time and was firing missiles and dropping bombs from manned aircraft.

In November, 2002, however, the CIA carried out the first killings using a drone far from the battlefields of Afghanistan. The attack occurred in Yemen where, at the time, no armed conflict was underway and no attack on the United States had occurred that could give rise to a U.S. right to undertake military action in Yemen. In 2004, the CIA began a campaign of targeted killing in Pakistan and, in late 2006, similar attacks began in Somalia. New drone bases are being established around the world, raising the expectation of future drone attacks. According to The Bureau of Investigative Journalism, by the end of 2013, the United States had killed as many as 4100 people beyond armed conflict zones with drones, including over 200 children.²⁷

The Obama Administration has tried to characterize these U.S. drone attacks as lawful by invoking as many as six distinct but contradictory justifications.²⁸ In an approach reminiscent of the legal argument made to justify the Cuban quarantine during the Cuban Missile Crisis and the use of force in the Kosovo intervention, the Administration's lawyers seem to pile on many arguments that might almost work in the hope that the public and allies might see the accumulated arguments as sufficient. These lawyers likely know that the arguments are not sufficient in international law but hope they will create a case of special circumstances that allows

27. *Monthly Updates on the Covert War*, BUREAU OF INVESTIGATIVE JOURNALISM, <http://www.thebureauinvestigates.com/category/projects/drones/monthly-updates/> (last visited Jan. 24, 2014).

28. Mary Ellen O'Connell, *Drone Attacks & International Law*, Address at the Indianapolis Peace and Justice Center (Nov. 26, 2013), *available at* http://indianapolis.granicus.com/MediaPlayer.php?view_id=51&clip_id=10804.

the United States, and perhaps a few close allies such as the UK and Israel, to use drones beyond armed conflict zones.

The U.S. position is, of course, untenable as a matter of law. Other countries are showing an interest in using drones in the same way the United States does, in particular, China. The *New York Times* carried a front-page article on the day these remarks were delivered, reading: “Hacking U.S. Secrets, China Pushes for Drones.”²⁹ China has apparently targeted companies that have developed U.S. drone technology with considerable success: “Chinese officials this month sent a drone near disputed islands administered by Japan; debated using a weaponized drone last year to kill a criminal suspect in Myanmar; and sold homemade drones resembling the Predator, the American model, to other countries for less than a million dollars each.”³⁰

The United States has set the precedent of using military force in situations in which, prior to 9/11, the United States would have used law enforcement methods. As a result, the legal and ethical barriers to resort to significant violence are being eroded. The United States is in the best position to slow this development by admitting its legal error and complying with its obligations. Only then will it be in position to protest China’s conduct or the conduct of other states.

CYBER WEAPONS

We have already discussed the Stuxnet worm as the first use of a computer program by one government to do significant physical damage to another. In January, 2010, investigators with the IAEA noticed something was wrong with the centrifuges at an Iranian nuclear facility. The Iranian scientists had been replacing the centrifuges at many times the normal rate.³¹ They discovered that, in 2009, someone had unleashed a program that had infiltrated computers across the world using the most complex malware ever written.³²

29. Edward Wong, *Hacking U.S. Secrets, China Pushes for Drones*, N.Y. TIMES, Sept. 21, 2013, at A1.

30. Edward Wong, *Hacking U.S. Secrets, China Pushes for Drones*, N.Y. TIMES (Sept. 20, 2013), http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?_r=0.

31. See Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July 11, 2011), <http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/>.

32. *Id.*

In response to the attack, Iran began recruiting its own team of elite hackers.³³ The goal was to prevent another attack and to gain the capacity to retaliate with a virus of its own. Something like a world arms race for cyber weapons may now be underway. The ability to keep the code for cyber weapons secret may prove even more difficult than keeping the secrets of nuclear, biological, and chemical weapons.³⁴ An adaptation of Stuxnet known as DuQu has already been created.³⁵ CrSyS, a lab of the Budapest University of Technology, discovered the program and wrote a sixty-page report on it.³⁶ CrSyS found it is “nearly identical to Stuxnet” but built for a different purpose.³⁷ DuQu was made to gather information,³⁸ specifically, to steal the blueprints of Iran’s nuclear program and then remove itself from Iran’s computers.³⁹ DuQu has also provided additional insight into the origins of Stuxnet. For example, researchers found that the Stuxnet’s working hours coincided with Jerusalem local time.⁴⁰

The invention of DuQu as a consequence of Stuxnet has not, apparently, deterred the United States. In 2012, another virus was detected, known as “Flame,” which appears to be a part of the same campaign as Stuxnet.⁴¹ A researcher at Kaspersky Labs, who brought Flame’s existence to public light, said, “We believe Flame was written by a different team of programmers but commissioned by the same larger entity.”⁴² Like DuQu, Flame is an espionage tool. It spreads through BlueTooth.⁴³ Also, like DuQu, Flame names many of its processes after American media characters, including BeetleJuice and Jason Bourne.⁴⁴ Virkram Thakur, a Symantec researcher, said, “This is the third such virus we’ve seen in the

33. Shaun Waterman, *Iran Ready to Launch Hacker Attacks on U.S. Infrastructure, Specialists Say*, WASH. TIMES (Apr. 25, 2012), <http://www.washingtontimes.com/news/2012/apr/25/iran-readying-hacker-attacks-us-infrastructure-spe/>.

34. Adam Levin, *Hackers: If You Can’t Beat ‘Em, Hire ‘Em*, ABC NEWS (June 16, 2012), <http://abcnews.go.com/Business/hackers-beat-em-hire-em/story?id=16578552>.

35. Kim Zetter, *DuQu Mystery Language Solved With the Help of Crowdsourcing*, WIRED (Mar. 19, 2012), <http://www.wired.com/threatlevel/2012/03/duqu-mystery-language-solved/>.

36. SYMANTEC SECURITY RESPONSE, W32.DUQU: THE PRECURSOR TO THE NEXT STUXNET (2011), available at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf.

37. *Id.* at 1.

38. Steven Cherry, *Hackers are Learning New Lessons from the Most Sophisticated Virus Code Ever Written*, IEEE SPECTRUM (Dec. 14, 2011), <http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet>.

39. Nicole Perlroth, *Researchers Find Clues in Malware*, N.Y. TIMES (May 30, 2012), <http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html>.

40. *Id.*

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.*

past three years. It's larger than all of them. The question we should be asking now is: How many more such campaigns are going on that we don't know about?"⁴⁵

Cyber weapons are very difficult to keep secret. Once they are decoded, they can be turned into new weapons. The Stuxnet virus was intended to target facilities with a specific layout.⁴⁶ However, it was spread using USB flash drives⁴⁷ and other means which have reached across the globe.⁴⁸

"[Stuxnet] spun out of control. Although it was intended to stop the progress of Iran's nuclear program, it also damaged 100,000 computers all over Europe. There was a need to stop it. Cyberwars act like boomerangs So it would be advisable for governments not to enter cyber-wars because in a boomerang war there are no winners."⁴⁹

Even if the United States and Israel used Stuxnet, it did not rise to the level of an armed attack that could trigger Iran's right to respond in self-defense by using force on the territory of the United States or Israel. Stuxnet did not meet the *Nicaragua* case test of a forceful or coercive action significant enough to be an armed attack.⁵⁰ Instead, it was a violation of the non-intervention principle.

International law raises substantial barriers to both using cyber weapons and defending cyberspace from cyber attacks through the use of military force. In general, international law supports regulating cyberspace as an economic and communications sphere and contains coercive means of responding lawfully to cyber provocations of all types. The same sort of coercive measures that are lawful to use against economic wrongs and violations of arms control treaties will generally be lawful to use in the case of a cyber attack. In the economic sphere, coercive responses to

45. *Id.*

46. Paul Mueller & Babak Yadegari, *The Stuxnet Worm* (University of Arizona Student Research Presentation), <http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf>.

47. *Id.*

48. *Stuxnet Goes Out of Control: Chevron Infected by Anti-Iranian Virus, Others Could Be Next*, RT (Nov. 9, 2012), <http://rt.com/usa/stuxnet-chevron-cyber-virus-348/>.

49. Ilan Gattegno, *Exclusive: Stuxnet Was Out of Control, We Had to Reveal It*, ISRAEL HAYOM (June 14, 2013), http://www.israelhayom.com/site/newsletter_article.php?id=9983.

50. The International Court of Justice has ruled on this very point in a number of important cases. See *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, 98–106 (June 27); *Armed Activities on the Territory of the Congo* (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, 222–3, 268 (Dec. 19).

violations tend to be known as “countermeasures”; in arms control, such countermeasures are commonly known as “sanctions.”

Whether designated countermeasures or sanctions, there are coercive enforcement measures not involving the use of significant military force available to states acting unilaterally in response to an internationally wrongful act.⁵¹ Despite the availability of these alternatives to the use of military force, it is important to reiterate that protecting cyberspace—keeping it viable for economic and communication uses—will generally require defensive measures, not offensive ones. Countermeasures are no substitute for good computer security.

When a state is the victim of a cyberattack or cyber espionage, and it has clear and convincing evidence that the wrong is attributable to a foreign sovereign state, the victim state may itself commit a wrong against the attacking state, so long as the wrong is commensurate with the initial wrong (proportionality) and aimed at inducing an end to the initial wrong (necessity) or the provision of damages. In most cases of cyber wrongs, the evidence that a foreign state is behind a particular act will come after the act is over or the damage is done. This fact indicates that most countermeasures aimed at cyber wrongs will aim at collecting money damages.

FULLY AUTONOMOUS ROBOTIC WEAPONS

The advent of robots with computer programs that can learn is triggering a new and intense discussion of the law and ethics around such weapons.⁵² Advances in artificial intelligence mean that once a robot is constructed and programmed, it will be able to make the decision to attack without additional human intervention.⁵³ Such an attack could occur years after the robot is programmed. The parties to the Convention on Certain Conventional Weapons⁵⁴ began a process in 2013 to study fully

51. Gabčíkovo-Nagymaros Project (Hung./Slovk.), 1997 ICJ REP. 7, 52–57 (Sept. 25).

52. U.S. Dep’t of Defense Directive 3000.09, *Autonomy in Weapon Systems* 2 (Nov. 21, 2012), available at <http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf> (“Autonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force.”); HUMAN RIGHTS WATCH, *LOSING HUMANITY: THE CASE AGAINST KILLER ROBOTS* (Nov. 2012), available at http://www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf.

53. Peter W. Singer, *In the Loop? Armed Robots and the Future of War*, BROOKINGS INST. (Jan. 28, 2009), http://www.brookings.edu/articles/2009/0128_robots_singer.aspx.

54. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Oct. 10, 1980, 1342 U.N.T.S. 137.

autonomous robotic weapons as the first step toward a new protocol controlling or prohibiting such weapons.⁵⁵ In April, 2013, UN Special Rapporteur Christof Heyns called for a moratorium on moving beyond the design stage in the development of fully autonomous weapons pending the formation of a panel of experts to “articulate a policy for the international community on the issue.”⁵⁶

BIOLOGICAL WEAPONS

Biological weapons have existed as long as warfare has. The modern word “toxin” derives from the Ancient Greek word for a poisoned arrow.⁵⁷ Early biological weapons “included the contamination of water with animal carcasses and filth.”⁵⁸ Some ancient military leaders used biological projectile weapons. For example, in a naval battle, Hannibal launched poisonous snakes onto enemy ships.⁵⁹ This tactic continued into the dark ages where armies flung plague victims into besieged cities.⁶⁰ European settlers in North America used smallpox as a biological weapon against the Native Americans. In the battle for Fort Pitt, one local militia leader wrote, “We gave them two Blankets and a Handkerchief from the Smallpox Hospital. I hope it will have the desired effect.”⁶¹ Similar tactics were used in the Ohio River Valley.⁶²

With the advent of scientific bacteriology in the nineteenth century, the world became more worried about the possibility of mass biological warfare. The Hague Conventions of 1899 and 1907 banned the use of “poison or poisoned arms.”⁶³ However, this measure did little to deter their

55. CAMPAIGN TO STOP KILLER ROBOTS, THE CONVENTION ON CONVENTIONAL WEAPONS AND FULLY AUTONOMOUS WEAPONS: BACKGROUND PAPER BY THE CAMPAIGN TO STOP KILLER ROBOTS (Sept. 26, 2013), available at http://www.stopkillerrobots.org/wp-content/uploads/2013/09/KRC_BackgrounderCCW_26Sep2013.pdf.

56. Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions*, U.N. Doc. A/HRC/23/47 (Apr. 9, 2013) (by Cristof Heyns).

57. James W. Martin et al., *History of Biological Weapons: From Poisoned Darts to Intentional Epidemics*, in MEDICAL ASPECTS OF BIOLOGICAL WARFARE 1, 2 (Zygmunt F. Dembek ed., 2007), available at https://ke.army.mil/bordeninstitute/published_volumes/biological_warfare/BW-ch01.pdf.

58. *Id.*

59. BRIG. GEN. J. H. ROTHSCHILD, TOMORROW’S WEAPONS: CHEMICAL AND BIOLOGICAL 12 (1964).

60. Martin et al., *supra* note 57, at 2.

61. E. WAGNER STEARN & ALLEN E. STEARN, THE EFFECT OF SMALLPOX ON THE DESTINY OF THE AMERINDIAN 45 (1945).

62. *Id.*

63. Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277, T.S.

use during the First World War. While both sides participated in biological warfare, the Germans led the effort. They started the first known state-sponsored biological research program,⁶⁴ and preemptively sent animals infected with anthrax to the United States and other countries.⁶⁵ Germany also attempted to destroy crops in Argentina using a fungus.⁶⁶

As a result of the failure of the 1907 Hague Convention to stop the use of these weapons (although perhaps it was more motivated by the use of chemical weapons to kill over 90,000 individuals in World War I), the 1925 Geneva Protocol banned the “use in war of asphyxiating, poisonous or other gasses, and of all analogous liquids, materials or devices.”⁶⁷ The treaty was credited with the prevention of the use of these weapons during World War II, but nevertheless had serious gaps in its coverage.⁶⁸ The parties reserved the right to use the weapons against non-parties; to use the weapons in retaliation; to stockpile, design, and test the weapons; and to limit the prohibition to wartime use.⁶⁹

Therefore, in the 1930s, Japan created a biological weapon program (eventually referred to using the unit references of the groups carrying out the research, Unit 731 and Unit 100). Japan’s program was on a far larger scale than Germany’s pre-World War I effort. More than 3000 Chinese prisoners were killed during testing.⁷⁰ Eleven Chinese cities were attacked during “field trials.” While these trials backfired on the Japanese (a number of their own citizens died in the process), an estimated 580,000 Chinese were killed.⁷¹ However, without an effective delivery system, the weapons were never deployed in war. The British also developed antipersonnel and anti-cattle biological weapons but never deployed them.⁷²

539. “In addition to the prohibitions provided by special Conventions, it is especially forbidden: (a) To employ poison or poisoned weapons.” *Id.* Regulations art. 23.

64. Martin et al., *supra* note 57, at 3.

65. Michael Jacobs, *The History of Biologic Warfare and Bioterrorism*, 22 *DERMATOLOGIC CLINICS* 231 (2004).

66. Martin et al., *supra* note 57, at 3.

67. Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, 94 L.N.T.S. 65.

68. Michael P. Scharf, *Clear and Present Danger: Enforcing the International Ban on Biological and Chemical Weapons Through Sanctions, Use of Force, and Criminalization*, 20 *MICH. J. INT’L L.* 477 (1999). See also *Chemical and Biological Weapons: Can they Be Eliminated or Controlled?*, 23 *C.Q. RESEARCHER* 1053 (2013).

69. Scharf, *supra* note 68, at 481.

70. Martin et al., *supra* note 57, at 3.

71. *Id.* at 4.

72. *Id.*

The United States took a defensive approach to biological warfare, focusing efforts on preventing an attack through President Roosevelt's War Reserve Service.⁷³ The United States did, however, give Japanese scientists amnesty in exchange for the data resulting from their atrocities. After the start of the Korean War, the United States developed its own anti-crop and antipersonnel weapons but never deployed them. Still, North Korean, Chinese, and Soviet officials have made numerous allegations against the United States.⁷⁴ However, these allegations were unsubstantiated, and the accusing countries refused offers by the ICRC and WHO to conduct investigations and thwarted a UN proposal to establish a neutral investigative body.⁷⁵

In 1972, as a result of the weak 1925 Geneva Protocol, the Biological Weapons Convention was adopted.⁷⁶ Under article I, parties agreed to never produce, stockpile, or otherwise acquire:

Microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes; [and] [w]eapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict.⁷⁷

Also, article II required the destruction of all such weapons.⁷⁸ It remains to improve the enforcement provisions of the treaty. Major efforts in this direction were made in the 1990s, and an on-site investigation capacity was proposed in

a protocol that envisioned states submitting to an international body declarations of treaty-relevant facilities and activities. That body would conduct routine on-site visits to declared facilities and could conduct challenge inspections of suspect facilities and activities as well.

73. *Id.* at 5.

74. *Id.* at 6.

75. *Id.* at 7.

76. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163.

77. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction art. I, Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163.

78. *Id.* art. II. See Susan Wright, *Prospects for Biological Disarmament in the 1990s*, 2 TRANSNAT'L L. & CONTEMP. PROBS. L. 453, 454 (1992).

However, a number of fundamental issues—such as the scope of on-site visits and the role export controls would play in the regime—proved difficult to resolve. In March 2001, the Ad Hoc Group’s chairman issued a draft protocol containing language attempting to strike a compromise on disputed issues. But in July 2001, at the Ad Hoc Group’s last scheduled meeting, the United States rejected the draft and any further protocol negotiations, claiming such a protocol could not help strengthen compliance with the BWC and could hurt U.S. national security and commercial interests.⁷⁹

CHEMICAL WEAPONS

The use of modern chemical weapons began in World War I. Robert O’Connell describes the moment:

Late in the afternoon on 22 April 1915 members of the French Forty-fifth (Algerian) and Eighty-seventh (Territorial) divisions were amazed to see a vast, greenish yellow cloud spring out of the ground and begin rolling toward their positions along the Ypres salient. Within moments the cloud had enveloped them, and they found themselves choking and fighting for breath. Those who were not immediately overcome ran in panic⁸⁰

The Allies had used some irritants earlier in the fighting, but the invention of a way to release bottled chlorine on the battlefield was a German scientific breakthrough. “[W]ithin a year the Allies would field workable chemical munitions of their own.”⁸¹ Both sides also quickly developed techniques and equipment for protecting their troops. To the extent the Germans tried to keep their chemical weapons technology secret or to stay ahead of the Allies, they failed. The Germans gained little or no advantage from their lead in developing chemical weapons. Already in 1925, the Geneva Gas Protocol came into force banning use of chemical weapons. The ban emerged from moral outrage, but took the form of a rule of international law. Then in 1993, the world adopted a comprehensive treaty declaring unlawful the use, production, and stockpiling of chemical weapons.

79. *The Biological Weapons Convention (BWC) at a Glance*, ARMS CONTROL ASSOCIATION, <http://www.armscontrol.org/factsheets/bwc> (last visited Jan. 26, 2014).

80. ROBERT O’CONNELL, *supra* note 8, at 252.

81. *Id.* at 253.

In addition to secrecy, we have examples of states attempting to use military force to stop the development of chemical weapons. In 2007, Israel bombed Syria aiming to end an alleged weapons program.⁸² Israel sent eight fighter jets to destroy an alleged secret weapons production facility Syria was building with assistance from North Korea. Reports stated that it was a nuclear weapons facility, but the facts indicate it was more likely a chemical weapons facility, specifically to manufacture nerve agents. Several days passed before Syria protested against the attack. It held back apparently to try to avoid drawing attention to its illicit activities.⁸³ Plainly this attack had little or no impact on Syrian chemical stockpiles, as chemical weapons have been used in the Syrian civil war that began in 2011.⁸⁴ The open question is whether Israel's attack explains why Syria did not join the Chemical Weapons Convention⁸⁵ in recent years despite indications from the UN Secretary-General that it was close to doing so.

In addition to Israel's actual use of unlawful force against Syria, the United States threatened to use force against Syria in August, 2013 following a use of chemical weapons during the civil war. The United States did not cite any basis in international law to justify such a use of force. Rather, references were made to the use of force in the Kosovo crisis in 1999. U.S. Ambassador to the UN Samantha Power, was asked on National Public Radio on September 9 whether a U.S. attack on Syria would be "legal." She answered that it would be a "legitimate, necessary, and proportionate response."⁸⁶

Ambassador Power's answer recalls a report Sweden commissioned following NATO's use of force against Serbia during the Kosovo crisis of 1999. The report's authors concluded that the seventy-eight days of bombing was unlawful under international law but, nevertheless,

82. See Ben Piven, *Timeline: Israeli Attacks on Syrian Targets*, ALJAZEERA (May 5, 2013), <http://www.aljazeera.com/indepth/features/2013/05/20135512739431489.html>.

83. See Mary Ellen O'Connell, *Affirming the Ban on Bombing Iran*, SYRACUSE L. REV. (2012), <http://www.law.syr.edu/student-life/publications/law-review/iran-nuclear-symposium/mary-ellen-oconnell.aspx>.

84. See U.N. Mission to Investigate Allegations of the Use of the Chemical Weapons in the Syrian Arab Republic, Rep. on the Allegations of the Use of Chemical Weapons in the Ghouta Area of Damascus, U.N. Doc. A/67/997 (Aug. 21, 2013).

85. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Jan. 13, 1993, 1974 U.N.T.S. 45.

86. Mark Memmott, *Strike on Syria: Meaningless Gesture or Necessary Response?*, NPR (Sept. 9, 2013), <http://www.npr.org/blogs/thetwo-way/2013/09/09/220611202/strike-on-syria-meaningless-gesture-or-necessary-response>.

“legitimate.”⁸⁷ In 2003, following the U.S.-led invasion of Iraq, the UN Secretary-General ordered a thorough review of the UN Charter rules on the use of force. The preliminary report of his High Level Panel concluded that, contrary to statements of some in the international law community that the use of force in Kosovo was “illegal but legitimate,” the measure of legitimacy in the international community is legality. It must be—law is the common code of all humanity. It is not the moral discernment of any particular national leaders.

Attacking Syria without Security Council authorization would violate law even more fundamental than the chemical weapons ban. Ambassador Power argued that because the Security Council will not authorize force, force must be used, lawful or not. She implies that force is the only way to keep important norms viable. Using force unlawfully, however, will only undermine the very system that also prohibits the use of chemical weapons.

It is important that a response be made to chemical weapons use, but the response needs to be a lawful response. As already discussed, international law has a variety of means, including countermeasures. Individual national leaders can be held accountable today for the use of chemical weapons. The International Criminal Court might have jurisdiction. Where it does not, the Security Council has established a variety of ad hoc criminal courts.

The Obama administration was aware that Syria was stockpiling chemical weapons and did not stop it. Interdicting such weapons would have been a lawful countermeasure in this case. An embargo kept Saddam Hussein from getting the inputs necessary to develop chemical, biological, and nuclear weapons programs. Having missed the opportunity to impose a similar embargo on Syria, the United States took the lead in the effort to destroy Syria’s chemical weapons stockpile and production facilities. The U.S. action is exemplary and should support the understanding that the use of chemical weapons is absolutely prohibited in international law. A use of force, on the other hand, would have violated a higher norm against military force to enforce another important norm. Such conduct would have been illogical and destructive of the normative system as a whole that has created the international consensus against chemical weapons use.

Political observers say the real focus of the threat of force against Syria was not Syria and chemical weapons, but Iran and nuclear weapons. That

87. THE INDEPENDENT INTERNATIONAL COMMISSION ON KOSOVO, THE KOSOVO REPORT (2001), available at <http://global.oup.com/academic/product/kosovo-report-9780199243099;jsessionid=32E75834D8BE857DD343D673C3C51981?cc=us&lang=en&>.

may be, but just as with Syria, for the United States to get Iran to comply with international legal obligations by threatening or actually violating international law undermines the U.S. case. The United States has been saying to Iran for many years that Iran is legally prohibited from possessing nuclear weapons under the NPT and that the UN Security Council has mandated UN weapons inspectors to have access to alleged nuclear sites. The U.S. ability to apply moral and legal suasion has been undermined in recent years owing to everything from the Guantanamo Bay prison, to the invasion of Iraq, to the use of drones. Bombing Syria over the use of chemical weapons would have been another significant violation of international law, likely with similar consequences.

CONCLUSION

In the last third of 2013, the art of diplomacy had a resurgence in the area of arms control. Thanks to a deftly negotiated agreement, Syria became committed to destroying its chemical weapons and joining the Chemical Weapons Convention. Soon after, Iran agreed to allow IAEA inspectors into its facilities and new negotiations were underway with the United States and others toward curtailing its nuclear program. Diplomacy, in contrast to secrecy or military force, has a proven record of success respecting arms control. In arms control, as in so much else, the past is prologue.