Cyberwar and International Law

By Luther Martin – ISSA member, Silicon Valley Chapter and Cheryl He

There is a lot of discussion of cyberwar these days, though much is not based on a careful understanding of what might reasonably be called "cyberwar." The authors look at what existing international law tells us about cyber attacks and at what recent cyber incidents might reasonably be considered to be serious enough to be considered something more than annoying attacks by hackers.

Abstract

There is a lot of discussion of cyberwar these days. Much of this discussion has one thing in common: it is not based on a careful understanding of what might reasonably be called "cyberwar." Here, we look at what existing international law tells us about cyber attacks and look at what recent cyber incidents might reasonably be considered to be serious enough to be considered something more than annoying attacks by hackers. This point of view both explains the limited nature of the damage caused by most cyber attacks that have occurred to date and lets us speculate on what the future will bring.

Armed conflict is surprisingly common. The "Global Peace Index 2016"[1] report by the Institute for Economics & Peace suggests that only 10 of the 163 countries for which they collect data are not participating in some sort of conflict today. Peace is very uncommon. As more participants in today's conflicts develop the capability to attack the computer systems of their opponents, it seems likely that more conflicts will involve some type of cyber attack.

Many cyber attacks to date have targeted civilian infrastructure rather than government systems and have stayed below a threshold that we will explain below, while the relatively low costs to their perpetrators have resulted in such attacks becoming increasingly common. Because any business may find itself as a target of cyber attack, they are a threat that CISOs should think about, and perhaps even plan for.

The law of war

There may have been rules to warfare for as long as men have been fighting wars. Some of the world's oldest literature describes rules that warring parties should follow.

In the *Mahabharata* (c. 1000 BC), Book 12, the "Book of Peace,"[2] lists rules for warfare, some of which should still sound reasonable to us today. It limits what weapons allowed in war: "There should be no arrows smeared in poison, nor any barbed arrows—these are the weapons of evil people." It has rules for treating the wounded: "One wounded should be given medical treatment in your realm; or he may even be sent to his own home." And it has rules for humane treatment of prisoners of war: "If [you have] captured a man who has discarded his sword, whose armor is broken to pieces, who pleads with his hands folded in supplication, saying, 'I am yours,' then [you] should not harm that man."

Today, the law of war comprises two bodies of law: one defines when the use of force is justified (*jus ad bellum*, Latin for "right to war"); the other governs how belligerents need to conduct themselves during a conflict (*jus in bello*, Latin for "right in war"). Here, we are not really interested in justifying starting cyber conflicts. That is not something that most corporate IT departments think about doing, so understanding the application of *jus ad bellum* to cyber conflicts is probably not important. But since it turns out to be easy for businesses to become involved in cyber conflicts, particularly as targets, understanding how *jus in bello* may apply is more interesting.

The *jus in bello* aspect of the law of war is currently defined by the four Geneva Conventions and three additional Proto-

1 "Global Peace Index 2016," Institute for Economics & Peace – http://visionofhumanity.org/app/uploads/2017/02/GPI-2016-Report_2.pdf.

2 Fitzgerald, James L., ed. *The Mahabharata, Volume 7*. University of Chicago Press, 2003.

cols[3] that were added after the last Convention was ratified. The Geneva Conventions were first ratified in 1864. They were updated in 1906, 1929, and finally in 1949. Since 1949, three additional Protocols have been ratified. Two were added in 1977 and a third in 2005.

Signatories of the Conventions and the additional Protocols agree to only engage in warfare within what is allowed by the Conventions and the additional Protocols. If an opponent violates the rules of warfare, the injured party is allowed to conduct reprisals, but they must be appropriate to the injury received. The legal concept of *lex talionis*, the law of proportionality, needs to cover any such reprisals.

Note that limits for what actions are allowed by participants in a conflict do not have to be formal laws or treaties. In the Cold War, espionage was carried out within a set of guidelines that both sides informally agreed to and generally followed.

Treaties and the prisoners' dilemma

A situation called the "prisoners' dilemma"[4] may explain why this is true. A prisoners' dilemma[5] is a situation when two or more parties will all benefit from cooperating, but each will individually benefit more from non-cooperation at the expense of the others. When this happens, we should expect all parties to choose to not cooperate with the others. An example of this is when two or more parties decide whether to obey a treaty or to cheat on it.

If all parties agree to not develop nuclear weapons, for example, then all parties are safer. But if one party cheats, it gains an advantage over the others who have not developed their own nuclear weapons. In this situation, we should expect all parties to cheat on a treaty that bans nuclear weapons, or, perhaps even more likely, to not agree to such a treaty in the first place. Thus all parties need an incentive to not cheat in order for rules, either formal or informal, to be generally followed.

Cyber weapons may offer compelling advantages. They are generally relatively inexpensive to develop compared to the cost of conventional weapons like tanks, aircraft, submarines, or aircraft carriers. The US Government Accountability Office (GAO) estimates that the US government will spend over $54 billion on the F-35 Joint Strike Fighter program between the years 2015 and 2019[6] and that the program will probably end up costing about $1.5 trillion over its complete life cycle (research, development, procurement, operation, maintenance, etc.).[7]

An investment of the same $54 billion over a five-year period in cyber weapon research is likely to result in weapons that are capable of both crippling the economies of many nations and rendering many modern weapon systems ineffective—something that even the very capable F-35 alone probably cannot do. And an investment of $1.5 trillion over a few decades might even produce cyber weapons that are closer to science fiction than to those that we see today. So the significant capabilities that they may provide at a relatively low cost may make cyber weapons seem compelling to both state and non-state actors.

It may be relatively easy to use such weapons against adversaries while still maintaining a plausible level of deniability due to the largely anonymous nature of the Internet. Cyber attacks can be far more humane than the alternatives. Crippling a country's banking infrastructure may cause a very high level of economic damage, but without the level of death and destruction that accompanies the use of conventional weapons.

Because of these advantages, the prisoners' dilemma may lead to the universal development of cyber weapons, perhaps even to a cyber arms race. Controlling these weapons will be problematic until both governments and non-government entities have a strong incentive to agree to limits on developing or using them. But it is also likely that the use of cyber weapons will be limited by the existing law of war, so indiscriminate and all-out cyberwar is probably unlikely.

The law of cyberwar

It may be useful to think of all conflicts involving two types operations: conventional and cyber. At one end of the spectrum we have operations that only use traditional forms of force, while at the other end are operations carried out purely through the use of computers. Conflicts can also exist somewhere between the two extremes, involving some conventional operations and some cyber operations. It is clear how the law of war limits acceptable behavior in purely conventional operations, but it turns out that the existing law of war also can be interpreted in a way that applies to cyber operations. The most notable discussion of this is contained in the *Tallinn Manual*.[8]

The *Tallinn Manual* was written between 2009 and 2012 by a group of subject matter experts in a project organized by the NATO Cooperative Cyber Defence Centre of Excellence[9] (CDCoE) (based in Tallinn, Estonia). The output of this project reflects the views of the contributors as to how well the existing law of war can be applied to cyberwar. The consensus of the experts was that the existing law of war can easily be interpreted in a way that applies to actions in cyberwar.

Of particular interest is the way that the *Tallinn Manual* describes what qualifies as "armed attacks" in the cyber world. This is particularly relevant because the term "act of war"

3 ICRC, "Geneva Conventions of 1949 and Additional Protocols, and their Commentaries" International Committee of the Red Cross – https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp.

4 Avinash Dixit and Barry Nalebuff, "Prisoners' Dilemma," Library of Economics and Liberty – http://www.econlib.org/library/Enc/PrisonersDilemma.html.

5 Tucker, Albert W. "The mathematics of Tucker: a sampler." *The Two-Year College Mathematics Journal* 14, no. 3 (1983): 228-232.

6 GOA, "F-35 Joint Strike Fighter: Assessment Needed to Address Affordability Challenges," US Government Accountability Office – http://www.gao.gov/products/GAO-15-364.

7 Joint Strike Fighter Program, "F-35 Lightning II Program Fact Sheet Selected Acquisition Report (SAR) 2015 Cost Data," US Department of Defense – http://www.jsf.mil/news/docs/20160324_Fact-Sheet.pdf.

8 Schmitt, Michael N., *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press, 2013.

9 NATO Cooperative Cyber Defence Centre of Excellence – https://ccdcoe.org/.

is a political term with no precise meaning, while the term "armed attack" has a clear legal definition. Treaties and similar agreements define what actions will be taken or can be taken in the event of an armed attack; they do not specify what actions can be taken in response to an act of war.

In particular, the *Tallinn Manual* uses the effects of a cyber attack to judge whether or not it qualifies as an armed attack. Cyber attacks that cause effects that are similar to what kinetic weapons (guns, bombs, etc.) cause count as the equivalent of an armed attack. Guns and bombs do not temporarily shut down banks or temporarily take down websites. They cause more physical and permanent damage. Many, perhaps even almost all, cyber attacks fall short of the *Tallinn Manual's* definition of armed attacks. This limits the options that national governments have for responding to these attacks, at least if they want to stay within the limits imposed by international law.

Estonia (2007)

In 2007, the government of Estonia decided to relocate the Bronze Soldier, a memorial to the victory of the Soviet Army over Nazi Germany. The government moved the memorial from a central location in the capital city of Tallinn to the nearby Tallinn Military Cemetery. This provoked riots in the streets of Tallinn. Soon, cyber attacks against many Estonian government and commercial targets were underway. Hackers carried out denial of service and distributed denial of service attacks against government and private-sector websites, including the those of the Riigikogu (Parliament), as well as the Estonian prime minister and president. Many government ministries, e-banking organizations, and news outlets also suffered attacks.

The effects of these attacks are not the same as would have been caused by kinetic weapons. It seems very likely that the cyber attacks that occurred in this incident did not qualify as armed attacks, so the government of Estonia and its allies would have been somewhat limited in their options for retaliating. In particular, any military action would almost certainly not have been justified in this particular case.

Stuxnet (2009)

While there are many descriptions of the Stuxnet worm and its effects, there are very few facts available concerning this incident. What we do know for sure is that some time in 2009 a worm appeared on the Internet that seemed to target ranges of IP addresses in Iran, and that this worm seemed to target certain industrial control systems—the centrifuges that were being used in uranium enrichment operations by the government of Iran.

Once it infected the control systems for the centrifuges, Stuxnet seemed to increase the rate at which centrifuges would spin, possibly causing damage to them by making them spin faster than they were meant to operate. This could potentially cause an increase in the failure rate of the centrifuges that could be very difficult to troubleshoot.

But essentially all that we know about Stuxnet is based on rumors. Many news stories have described in detail how the governments of the US, Israel, and Germany worked together to create and deploy Stuxnet. And many news stories and other reports have explained how the effects of Stuxnet delayed the Iranian nuclear program by degrading its ability to refine fissionable isotopes of uranium. But there are few, if any, facts to support these entirely plausible conclusions. A good summary of what is really known about Stuxnet and its effects is contained in the NATO CDCoE report "Stuxnet – Legal Considerations," by Katharina Ziolkowski.[10]

None of the governments of the US, Israel, or Germany has officially admitted to taking part in the development or deployment of Stuxnet. And the government of Iran has never officially admitted that any of the centrifuges used in their nuclear program were damaged by Stuxnet.

There is no hard evidence that Stuxnet had any significant effect at all.

There is no hard evidence that Stuxnet had any significant effect at all. The centrifuges used in the Iranian nuclear program were notoriously prone to failure,[11] and it is not clear that the number of centrifuges bought by the Iranian government increased after Stuxnet appeared on the Internet, suggesting that it might not have significantly affected the Iranian nuclear program at all.

In the absence of any reliable information, it is hard to judge whether or not Stuxnet was damaging enough to qualify as the equivalent of an armed attack, but Ziolkowski's legal analysis suggests that it was not just a clever bit of technology. Stuxnet was carefully tailored to keep its effects from violating international law, which could have justified any possible retaliation by Iran: "Under the supposition that the malicious software has been created, installed, and controlled by one or more States and indeed did not cause any damage of physical nature, it appears not to reach the threshold of illegality pursuant to public international law and thus to be a 'legal masterpiece.'"

So the best information available suggests that Stuxnet probably did not cause enough damage to qualify as an armed attack. This means that the government of Iran probably would not have been justified in using armed force to retaliate against one or more countries that it might have suspected carried out the Stuxnet attack.

German steel mill (2014)

In December 2014, the German government's Bundesamt für Sicherheit in der Informationstechnik (BSI) (Federal Office for Information Security) released their annual findings report "Die Lage der IT-Sicherheit in Deutschland 2014" ("The State of IT Security in Germany 2014").[12] This report describes a successful cyber attack on an unspecified German steel mill, although it provides few details. This attack apparently compromised the control systems for the steel mill and resulted in significant physical damage to at least one of the blast furnaces used in the mill.

Of all of the cyber attacks publicly known, this attack seems to come the closest to counting as an armed attack because there was significant physical damage caused by it. While the damage caused may not have been exactly like the damage that would have been caused by guns or bombs, it was probably very similar. It might have been similar enough to the effect of kinetic weapons to have counted as the equivalent of an armed attack.

Because there have been very few cyber attacks that cause significant physical damage, it may be the case that this particular cyber attack is the only attack to date that might reasonably be considered to be equivalent to an armed attack; it is also the only one that might reasonably be considered serious enough to justify a military response by the affected country.

Summary

There are compelling reasons why participants in twenty-first century conflicts would engage in cyberwarfare. Cyber weapons are almost certainly much less expensive to develop and use than conventional weapons, and the anonymity provided by the Internet can make it extremely hard to reliably identify exactly who carried out a cyber attack. Launching damaging cyber attacks against government or military targets will almost certainly be regarded as an act of war by politicians, so many participants in the cyber attacks have largely restricted their attacks to non-government and non-military targets. Cyber attacks have generally not caused the type of physical damage that might classify them to being equivalent to an armed attack, thus limiting the ways in which governments can respond. If this trend continues in the future, businesses may unwillingly become targets in cyber conflicts.

So it certainly looks like businesses are on the front lines of cyberwar, whether they want to be or not. A reasonable precaution is thus to hope for the best (not being the target of a cyber attack) but to be prepared for the worst (that you will end up being the target of a cyber attack).

About the Authors

Luther Martin is a Distinguished Technologist at Micro Focus. You can reach him at luther.martin@microfocus.com.

Cheryl He is a Software Engineer at Hewlett Packard Enterprise. You can reach her at cheryl.he@hpe.com.

10 Dr. iur. Katharina Ziolkowski, "Stuxnet–Legal Considerations," NATO CCDCoE (2012) - https://ccdcoe.org/sites/default/files/multimedia/pdf/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf.

11 Greg Thielmann and Peter Crail, "Chief Obstacle to Iran's Nuclear Effort: Its Own Bad Technology," The Christian Science Monitor, Dec. 8, 2010 –http://www.csmonitor.com/Commentary/Opinion/2010/1208/Chief-obstacle-to-Iran-s-nuclear-effort-its-own-bad-technology.

12 "Die Lage der IT-Sicherheit in Deutschland 2014," Bundesamt für Sicherheit in der Informationstechnik – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile.