INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1901
U.S. NAVAL WAR COLLEGE

Methods and Means of Cyber Warfare

William H. Boothby

89 INT'L L. STUD. 387 (2013)

Volume 89 2013

Methods and Means of Cyber Warfare

William H. Boothby[*]

I. WHAT IS A CYBER WEAPON?

Central to the conduct of hostilities in an armed conflict are the tools and techniques with which the fight is undertaken. In non-cyber warfare, the tools, that is, the missiles, bombs, rifles, bayonets, mines, bullets and other weapons and associated equipment, are employed in ways that differ according to the military purpose that it is being sought after. These twin ideas of "military tools" and of the ways in which they are employed can be applied equally to cyber warfare. It follows that we should consider how the law that regulates, respectively, the tools or means of warfare and the ways or methods whereby those tools are used should properly be applied in the cyber context.

Any discussion of cyber methods and means of warfare should take as its starting point the more general notion of means and methods of warfare. Means of warfare consist of all weapons, weapons platforms and associated equipment used directly to deliver force during hostilities. Methods of warfare consist of the ways in which weapons are used in hostilities.

Weapons are devices, munitions, implements, substances, objects or pieces of equipment which generate an offensive capability that can be ap-

* Air Commodore, Royal Air Force (Ret.).

plied to an enemy person or object.[1] The *Manual on the Law of Air and Missile Warfare* (*AMW Manual*) defines the term "weapon" as "a means of warfare used in combat operations, including a gun, missile, bomb or other munitions, that is capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects."[2] The accompanying commentary makes the point that the force used need not be kinetic, citing the effects produced by certain computer network operations.[3] In its Glossary of Military Terms, the U.S. Department of Defense defines a weapon system as "[a] combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery or deployment (if applicable) required for self-sufficiency."[4] The *AMW Manual* characterizes "means of warfare" as "weapons, weapon systems or platforms employed for the purposes of attack"[5] with the result that means of warfare involves not just weapon systems, but also equipment used to control, facilitate or direct the conduct of hostilities.[6]

Weapons as conventionally understood can take a variety of forms. While some weapons, such as bombs, rockets, bullets, artillery shells and the like generate their destructive effect by the use of kinetic force, other kinds of weapons, such as gases, chemical and biological agents achieve

1. WILLIAM H. BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 4, 344 (2009).

2. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rule 1(ff) (2009). The Program on Humanitarian Policy and Conflict Research at Harvard University (HPCR) convened a group of international legal experts to review and restate the existing law of air and missile warfare. At the end of a multi-year process HPCR published the *Manual on International Law Applicable to Air and Missile Warfare*, which contains the black-letter rules reflecting the overall consensus of the legal experts of the existing law of international armed conflict bearing on air and missile warfare. HPCR also published the COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2010) [hereinafter AMW COMMENTARY]. In the *Commentary* each Black-letter Rule is accompanied by a commentary intended to provide explanations of the rule. For ease of citation, citations in this article will be to the *Commentary* since it contains both the rules and their associated commentary.

3. AMW COMMENTARY, *supra* note 2, rule 1(ff) cmt. ¶ 1, at 55.

4. Joint Chiefs of Staff, Joint Publication 1-02, DOD Dictionary of Military and Associated Terms (Nov. 8, 2010), as amended through July 15, 2012, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

5. AMW COMMENTARY, *supra* note 2, rule 1(t), at 41.

6. *Id.*, rule 1(ff) cmt. ¶ 3, at 55.

their wounding or deadly purpose without necessarily operating kinetically.[7] The critical factor in relation to all weapons is the injurious or damaging effect that they have on the persons and/or objects associated with the adverse party to the conflict.

Applying these notions in the cyber domain, the immediate question is how a cyber capability resident, for example, on a thumb drive that is released by simply pressing the "enter" key can possibly be described as an offensive capability, thus, potentially, as a cyber weapon. As Professor Schmitt has pointed out, it is the violent consequences that are designed or intended to follow the use of the cyber capability that are critical to the characterization of such a cyber event as a cyber attack. The same intended violent consequences are critical to the characterization of a cyber capability as a cyber weapon.[8] Therefore, a cyber weapon would comprise any computer equipment or computer device that is designed, intended or used, in order to have violent consequences, that is, to cause death or injury to persons or damage or destruction of objects.

"Object" denotes any physical object, such as a piece of computing equipment. If the cyber capability burns out components in the targeted computer system, the requirement as to damage will be satisfied. Equally, the effect of the cyber capability on the facility which the targeted computer serves may render the capability a cyber weapon. For example, the object against which the cyber operation is directed is the supervisory control and data acquisition system that controls the operation of a public utility installation, such as a water treatment works, or, a similar computer system that controls a production process, such as at an oil refinery. In these cases the damage that is caused by the cyber operation to the water treatment installation or to the oil refinery will also cause the cyber tool to be considered a cyber weapon.

The next question is whether damage to data within a computer system that does not affect the facility or service that the targeted computer system provides constitutes damage for these purposes. In other words, is the data resident in the target computer system to be regarded as an object? The author's view is that such data only becomes an "object" when it is critical

7. While it is well appreciated that the listed weapons are generally prohibited by treaty, it is the fact that they are nevertheless widely recognized as weapons that is critical here.

8. Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, *in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89, 93–94 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies).

to the operation of the targeted system.[9] If as a result the targeted computer ceases to perform the required control function causing, in our examples, water purification or oil refining to cease, this would amount to damage if repairs are needed before production can resume. A cyber tool being used for such a purpose would, therefore, be a cyber weapon. Temporary shutdown causing inconvenience or irritation would not amount to damage or injury, and use of a cyber tool to cause those results would not cause it to be regarded as a cyber weapon.[10]

If, in considering these principles, we conclude that a particular cyber tool has an offensive capability, the remaining issue is whether it can properly be described as "applied" to an enemy person or object. There is an inherent indirectness about cyber activity in which there are often numerous orders of effect. The first order of effect is the direct impact of the cyber activity on the data in the targeted computer. That produces the second order effect by affecting the service the target computer provides. The resulting damage, injury and other consequences that the termination or interruptions of service cause to the customers of the targeted computer system constitute third order effects, which may well have been the main purpose in undertaking the cyber operation. Computer linkages and customer dependencies taken together comprise the mechanism that is being exploited to apply the offensive cyber capability—or cyber tool—to the targeted object or person. Indeed, that cyber tool can properly be regarded as applied to all of the devices, data, objects and persons within this chain of effect.

We can therefore properly conclude that computers, computer data and associated mechanisms that are capable of generating any of these orders of effect on an adverse party to the conflict are capable of being a cyber weapon. Such computers, data or mechanisms will only actually become a cyber weapon, however, if they are used, designed or intended to be used for such purposes.[11]

---

9. *See also* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE rule 38 cmt. ¶ 5 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

10. For a discussion of these issues in relation to the notion of cyber attack, see KNUT DÖRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS 6 (2004), *available at* http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/68lg92?opendocument (paper delivered at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm); Schmitt, *supra* note 8, at 95.

11. A distinction must therefore be drawn between the use of cyber capabilities for offensive purposes, as discussed in this section of the article, and their use, for example,

II. FUNDAMENTAL PRINCIPLES OF WEAPONS LAW

The customary, fundamental principles and established rules of weapons law apply to cyber weapons no less than any other weapons. As the International Court of Justice observed in the *Nuclear Weapons* advisory opinion,

> the intrinsically humanitarian character [of the established principles and rules of humanitarian law applicable in armed conflict] permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.[12]

There are three customary principles of weapons law. The first is that the right of the parties to an armed conflict to choose methods or means of warfare is not unlimited.[13] This means that those involved in undertaking cyber operations during armed conflicts have a clear legal duty to "respect the rules of international law applicable in case of armed conflict."[14]

By the second customary principle, it is "prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering."[15] The injury and suffering to

---

for information gathering or espionage. While a cyber capability may be capable of generating the stated orders of effect, thereby causing death, injury, damage or destruction, it is only if it is used to cause these things that it will become a weapon. While the logic leading to this conclusion seems to the author to be inescapable, consider, however, the valid issues raised in Duncan Blake & Joseph S. Imburgia, *Bloodless Weapons? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons,"* 66 AIR FORCE LAW REVIEW 157 (2010).

12 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 86 (July 8), *reprinted in* 35 INTERNATIONAL LEGAL MATERIALS 809 (1996).

13. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 35(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

14. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 1404 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987). Note also the Martens clause at Additional Protocol I, art. 1(2), *supra* note 13 ("In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.").

15. Additional Protocol I, *supra* note 13, art. 35(2). The original U.S. Department of Defense weapons review directive was prepared by Edward R. Cummings, Waldemar A. Solf and Harry Almond. They included in the document what the author regards as the most clear and accurate formulation of the superfluous injury and unnecessary suffering

be assessed in the case of cyber weapons is that expected under each of the orders of effect that were described in the previous section. In applying this rule, the legitimacy of a cyber weapon must be assessed "by comparing the nature and scale of the generic military advantage to be anticipated from the weapon in the application for which it is designed to be used with the pattern of injury and suffering associated with the normal, intended use of the weapon."[16] The references to the generic nature of the military advantage and to the injury and suffering associated with normal use make the point that this test is mainly concerned with the generality of such aspects and not with the circumstances on a particular occasion. It is the qualities of the weapon per se, rather than the particularities of a specific attack, with which the weapons law test is usually concerned. If, however, as will frequently be the case, a cyber weapon is being prepared or procured in order to be used on a known occasion against a specified target, the ad hoc circumstances must be carefully considered when determining whether the superfluous injury/unnecessary suffering test is satisfied.[17]

---

test currently available. The test is lengthy but is reproduced here because of its clarity and relevance.

> The prohibition of unnecessary suffering constitutes acknowledgment that necessary suffering to combatants is lawful, and may include severe injury or loss of life. There is no agreed international definition for unnecessary suffering. A weapon or munition would be deemed to cause unnecessary suffering only if it inevitably or in its normal use has a particular effect and the injury caused is considered by governments as disproportionate to the military necessity for it, that is, the military advantage to be gained from its use. This balancing test cannot be conducted in isolation. A weapon's or munition's effects must be weighed in light of comparable, lawful weapons or munitions in use on the modern battlefield. A weapon is not unlawful merely because it may cause severe suffering or injury. The appropriate determination is whether a weapon's or munition's employment for its normal or expected use would be prohibited under some or all circumstances. The correct criterion is whether the employment of a weapon for its normal or expected use inevitably would cause injury or suffering manifestly disproportionate to its military effectiveness.

This text is reproduced in W. Hays Parks, *Means and Methods of Warfare,* 38 GEORGE WASHINGTON INTERNATIONAL LAW REVIEW 511, 517 n.25 (2006). *See also* MICHAEL BOTHE, KARL JOSEF PARTSCH & WALDEMAR A. SOLF, NEW RULES FOR VICTIMS OF ARMED CONFLICTS, COMMENTARY ON THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949, at 200–201 (1982).

16. William J. Fenrick, *The Conventional Weapons Convention: A Modest but Useful Treaty*, 279 INTERNATIONAL REVIEW OF THE RED CROSS 498, 500 (1990); BOOTHBY, *supra* note 1, at 63.

17. Accordingly, when a cyber weapon is being developed for use against a known target, it is the injury to persons that is to be expected as a result of the way it is to be used on that occasion against the intended target that must be compared with alternative methods of achieving the desired military purpose in order to determine whether the cyber

The third customary principle of weapons law is that it is prohibited to employ weapons, means or methods of warfare, including cyber weapons, which are indiscriminate by nature. This rule, derived from Article 51(4) of the 1977 Additional Protocol I (AP I) to the four 1949 Geneva Conventions, has customary law status, thus binding all States.[18] If the cyber weapon cannot be directed at a particular military objective or if its effects cannot be controlled, it will likely breach this weapons law part of the discrimination rule.[19]

This rule would seem to be particularly relevant to cyber weapons. Thus, if the characteristics of a piece of cyber malware are such that it will cause damage to the target computer system, but also infect and damage numerous other civilian computer systems or websites, the cyber weapon may be indiscriminate by nature and prohibited by the rule. The critical issue here is whether the cyber weapon not only engages the intended target, but also reasonably limits its damaging effect to that intended target.

An attack that breaches the proportionality rule in Article 51(5)(b) of AP I is an example of an attack that would breach the indiscriminate attacks prohibition.[20] In the cyber context, it will not be the only example.

---

weapon, means or method of warfare is of a nature to cause superfluous injury or unnecessary suffering.

18. Having noted that indiscriminate attacks are prohibited, the paragraph so far as relevant, defines indiscriminate attacks as

> (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by [the] Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

Additional Protocol I, *supra* note 13, art. 51(4). The V2 rockets used by Germany towards the end of World War II are the sort of weapon that would have breached this rule. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 14, ¶ 1958. On the rule generally, see Michael N. Schmitt, *Future War and the Principle of Discrimination*, 28 ISRAEL YEARBOOK ON HUMAN RIGHTS 51, 55 (1998).

19. The UK *Manual* observes, "It is prohibited to employ weapons which cannot be directed at a specific military objective or the effect of which cannot be limited as required by Additional Protocol 1 and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction." UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 6.4 (2004) [hereinafter UK MANUAL].

20. Article 51(5)(b) of Additional Protocol I provides that the following type of attack is to be considered indiscriminate, namely an attack "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination

Other examples may include worms, viruses and other malware whose nature is to spread their effects uncontrollably, and cyber malware that, though it is designed to attack only the targeted computer node, is also of a nature to cause incidental second and/or third order damage to civilian users[21] of the target computer system, including those who may not necessarily be known to the targeteer.

The execution of discriminating cyber attacks therefore presupposes that the weapon system to be employed is capable of reasonably limiting its effects to the target computer system and to the targeted customers of that system. This is the first matter to consider when determining whether the cyber weapon is indiscriminate by nature. If it passes that test, the planned operational procedures must adequately inform the assessment whether any particular planned attack will be discriminating. Information will be required as to the target system, its linkages, its dependencies and its customers and as to the customers of any linked system that is also liable to be affected by planned cyber attacks. Planning such attacks will place considerable demands on intelligence resources. Additionally, as will be addressed in the weapons review section below, the reviewer conducting the required legal review will wish to be satisfied that the broader context in which the cyber weapon will be used is not such as to render its nature indiscriminate.

III. SPECIFIC WEAPONS LAW RULES OF RELEVANCE TO CYBER WEAPONS

Some of the technology-specific weapons law rules would seem to be of particular potential relevance to cyber warfare; these are discussed in this section.

Two sets of rules protect the natural environment during armed conflict. Article 35(3) of AP I prohibits the employment of "methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment."[22] By contrast,

---

thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

21. The word "users" is here intended to include not only persons but systems or objects that would suffer injury, death, damage or destruction.

22. Note that Article 55 of Additional Protocol I additionally requires that care be taken in warfare to protect the natural environment against widespread, long-term and severe damage, such protection to include a prohibition "of the use of methods or means of warfare which are intended or may be expected to cause such damage to the natural environment and thereby to prejudice the health or survival of the population."

the 1976 UN Environmental Modification Convention[23] addresses the use of the environment as a weapon. Its core provision is an undertaking by States party "not to engage in military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other state party."[24] The Convention defines "environmental modification techniques as "any technique for changing—through the deliberate manipulation of natural processes—the dynamics, composition or structure of the Earth, including its biota, lithosphere, hydrosphere and atmosphere, or of outer space."[25]

The effect of these rules is that any cyber weapon, the second and third order effects of which can be expected to be widespread, long-term and severe damage to the natural environment, will be prohibited and should not be used. Equally, the use of cyber methods alone, or perhaps more likely in association with the use of a conventional weapon or substance of some type, to achieve the defined forms of environmental modification and which cause injury, damage or destruction to an opposing party to the conflict is also prohibited. A cyber weapon designed to cause the core of a nuclear electricity generating station to ignite, thereby spreading high levels of long-lasting nuclear contamination that renders wide areas of surrounding territory uninhabitable for very protracted periods, is likely to be an example of a cyber weapon that would breach the AP I rule.

The use of poisons, poisoned weapons and asphyxiating gases is prohibited at customary law and by treaty provision.[26] Biological weapons are

---

23. Convention on the Prohibition of Military or Any Hostile Use of Environmental Modification Techniques, May 18, 1977, 31 U.S.T. 333, 1108 U.N.T.S. 151 [hereinafter ENMOD Convention] For a discussion of ENMOD, see Arthur H. Westing, *The Environmental Modification Convention of 1977—Reflections in Anticipation of the Second Review Conference*, 5 HUMANITÄRES VÖLKERRECHT INFORMATIONSSCHRIFTEN 70 (1992); ENVIRONMENTAL WARFARE: A TECHNICAL, LEGAL AND POLICY APPRAISAL (Arthur H. Westing ed., 1984); Jozef Goldblat, *The ENMOD Convention: A Critical Review*, 2 HUMANITÄRES VÖLKERRECHT INFORMATIONSSCHRIFTEN 82 (1993).

24. ENMOD Convention, *supra* note 23, art. I(1).

25. *Id.*, art. II(1).

26. The customary prohibition on the use of poison and poisoned weapons is reflected in Article 23(a) of the 1907 Hague Regulations. Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2227. *See also* UK MANUAL, *supra* note 19, ¶ 6.19.1; 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW rule 72 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005). The prohibition of the use of asphyxiating gases is set out in the 1925 Geneva Gas Protocol and is binding as customary law.

prohibited by the 1972 Biological Weapons Convention[27] and chemical weapons are prohibited by the 1993 Chemical Weapons Convention.[28] The possession or use of biological weapons is, in the author's view, prohibited by customary law, while the prohibition on use of chemical weapons is fast becoming a customary rule, if indeed it has not already achieved that status.[29] A cyber weapon will not generally have the nature of a poison, gas, chemical or biological weapon. However, cyber operations may enable a party to the conflict to gain effective control over such weapons or substances from an adverse party to the conflict. If a State's use of cyber methods results in it gaining control of poisons, poisoned weapons, asphyxiating gas, chemical weapons or biological weapons from an opposing party, it may not employ cyber or other methods to use such weapons or substances in connection with the armed conflict. It must take action to safeguard and, in the case of chemical and biological weapons, to destroy them to the extent that its degree of control and other factors enable it practically to do so.[30]

Protocols adopted under the aegis of the Convention on Certain Conventional Weapons (CCW)[31] address a number of classes of weapon. Protocol I prohibits weapons "the primary effect of which is to injure by fragments which in the human body escape detection by X-rays."[32] It

---

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, *reprinted in* 14 INTERNATIONAL LEGAL MATERIALS 49 (1975).

27. 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 [hereinafter Biological Weapons Convention]. For a discussion of the convention, see Josef Goldblat, *The Biological Weapons Convention—An Overview*, 318 INTERNATIONAL REVIEW OF THE RED CROSS 251 (1997).

28. 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.

29. See discussion in BOOTHBY, *supra* note 1, at 129, 137.

30. Note that the destruction obligations in the Biological Weapons Convention extend to weapons that a State party to the treaty possesses or controls. Biological Weapons Convention, *supra* note 27, art. II. It will be a matter of interpretation whether cyber operations have the effect of placing chemical or biological weapons under the control of a State party to the relevant Convention. If they do have that effect, the obligations in the relevant Convention addressed to a State having control of such a weapon must be considered.

31. 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.

32. Protocol on Non-Detectable Fragments, Oct. 10, 1980, 1342 U.N.T.S. 168.

would seem most unlikely that a cyber weapon would be designed or intended to have a second or third order effect of releasing a weapon with such characteristics. Protocol II and the amended version of the Protocol will be considered below. Protocol III[33] imposes prohibitions and restrictions on the use of incendiary weapons as defined in Article 1 of the Protocol. It is prohibited to make a military objective located within a concentration of civilians the object of attack by air-delivered incendiary weapons. A similarly located military objective may only be made the object of attack by a non-air-delivered incendiary weapon if the military objective is clearly separated from the concentration of civilians, and all feasible precautions are taken to limit the incendiary effects to the military objective and avoid or minimize incidental civilian injury and loss.

Protocol IV[34] to the CCW prohibits laser weapons specifically designed as one of their combat functions to cause permanent blindness to unenhanced vision.[35] If a laser weapon has the potential to cause such blindness, it would be unlawful to use in conjunction with that weapon a cyber tool that is intentionally designed to cause permanent blindness. For example, a cyber tool designed to direct the laser beam towards the line of sight of enemy personnel would be prohibited.

Mines[36], booby-traps[37] and other devices[38] are regulated by Protocol II[39] and Amended Protocol II to the CCW. Anti-personnel mines are prohibit-

---

33. Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons, Oct. 10, 1980, 1342 U.N.T.S. 171.

34. Protocol on Blinding Laser Weapons, Oct. 13, 1995, 1380 U.N.T.S. 370.

35. *Id.*, art. 1. Article 4 defines permanent blindness.

36. "'Mine' means a munition placed on, under or near the ground or other surface area and designed to be exploded by the presence, proximity or contact of a person or vehicle." Amended Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices art. 2(1), May 3, 1996, 2048 U.N.T.S. 93 [hereinafter CCW Amended Protocol II].

37. "'Booby-trap' means any device or material which is designed, constructed or adapted to kill or injure and which functions unexpectedly, when a person disturbs or approaches an apparently harmless object or performs an apparently safe act." *Id.*, art. 2(4).

38. "'Other' devices means manually emplaced munitions and devices including improvised explosive devices designed to kill, injure or damage and which are actuated manually, by remote control or automatically after a lapse of time." Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices art. 2(3), Oct. 10, 1980, 1342 U.N.T.S. 168 [hereinafter CCW Protocol II]. Note the developed definition of the same term for the purposes of Amended Protocol II, namely, "'Other devices' means manually-emplaced munitions and devices including improvised explosive devices de-

ed by the 1997 Ottawa Convention.[40] The references to "exploded" and to munition placement in the CCW mine protocols lead to the common sense conclusion that a purely cyber weapon cannot be a mine. For similar reasons, a purely cyber weapon cannot be an anti-personnel landmine within the meaning of the Ottawa Convention.[41]

However, the CCW Protocol II definition of booby-trap refers to "any device or material," notions that would seem to be broad enough potentially to include a cyber device. If a cyber device were, for example, to take the form of a kill switch embedded in a piece of malware planted by cyber means into the target computer system and which operates unexpectedly when a user of the targeted computer system undertakes a usually safe task such as switching on the computer, there is the potential for the cyber device to come within the Protocol II definition of booby-trap.[42] The cyber device is only capable of being a booby-trap, however, if it is "designed, constructed or adapted to kill or injure." If malware comprising a kill switch is designed to disable, say, the electricity supply to facilities that are essential to life support, it would be a matter of national interpretation whether this amounts to designed, constructed or adapted to kill or injure. While death or injury may be the intended second or third order effect of such a device, States may take the view that only devices that kill or injure as the immediate, or first order effect, come within the Protocol II definition. A less restrictive view would, however, see certain cyber capabilities as coming within the definition of booby-trap, with the result that Articles 3, 7, 9 to 14 and elements of the Technical Annex to the treaty would apply to such cyber weapons.[43] Article 7 would specifically prohibit the use of such booby-traps in any way associated with the objects listed in paragraph (1).[44]

---

signed to kill, injure or damage and which are actuated manually, by remote control or automatically after a lapse of time." CCW Amended Protocol II, art. 2(5).

39. CCW Protocol II, *supra* note 38.

40. Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction, Sept. 17, 1997, 2056 U.N.T.S. 211.

41. *Id.*, art. 2 (defines anti-personnel mines as meaning mines "designed to be exploded" by specified events).

42. TALLINN MANUAL, *supra* note 9, rule 44.

43. A similar definition of booby-trap appears in Article 2(2) of CCW Amended Protocol II. A State party that takes the view that a cyber weapon comes within the definition would apply Articles 3, 4 and 6–9.

44. The listed objects are internationally recognized protected emblems, signs or signals; sick, wounded or dead persons; burial or cremation sites or graves; medical facilities,

The Protocol II definition limits "other devices" to "manually emplaced munitions and devices." This would seem to exclude devices that are emplaced by remote means, such as by email. If, however, a thumb drive bearing the malware were to be manually inserted into the target computer system, it would be a matter of national interpretation whether this amounts to "manual emplacement" for the purposes of Protocol II and Amended Protocol II. It may be reasonable for States to conclude that the cyber weapon is distinct from the gadget that is used to transport it, and to decide that the thing being manually emplaced is the thumb drive, as opposed to the cyber weapon that it contains. Such an approach would suggest that a cyber weapon is not capable of being an "other device" for the purposes of those treaties.[45]

If a State's use of cyber methods enables it to take control of minefields, booby-traps or "other devices" from an opposing party, it may only use such weapons in accordance with the relevant treaty rules to which it is subject. If, however, a computer control system associated with a minefield, booby-trap or other device were to be transferred into the control of another party to the conflict as a result of a cyber operation, it would be a matter of interpretation whether that party had a sufficient degree of control over them for the Protocol II, Amended Protocol II and/or Ottawa Convention obligations to arise.

Where cluster munitions are concerned, a State that is party to the Convention on Cluster Munitions[46] and which, by cyber means, takes control of the cluster munitions of an adverse party to the conflict may not use such cluster munitions in breach of its own treaty obligations. It must also take action to safeguard and destroy them to the extent that its degree of control and other factors make it practicable to do so.

---

medical equipment, medical supplies or medical transportation; children's toys or other portable objects or products specially designed for the feeding, health, hygiene or clothing or education of children; food or drink; kitchen utensils or appliances except in military establishments, military locations or military supply depots; objects clearly of a religious nature; historic monuments, works of art or places of worship which constitute the cultural or spiritual heritage of peoples; or animals or their carcasses.

45. The corresponding definition in Article 2(3) of CCW Amended Protocol II is expressed in similar, but not identical, terms so it would be equally respectable to conclude that a cyber weapon is not capable of being an "other device" for the purposes of the amended Protocol.

46. Convention on Cluster Munitions, *opened for signature*, Dec. 3, 2008, *reprinted in* 48 INTERNATIONAL LEGAL MATERIALS 357 (2008). "Cluster munition" is defined by Article 2 of the Convention.

The discussion in this section is not intended to be an exhaustive treatment of all of the rules of weapons law that may potentially be of relevance in the cyber context. Rather it is intended to illustrate how cyber activity may either constitute activity that is covered by a weapons law provision or may, because of the control being exercised over an adverse party's weapon, give rise to weapons law responsibilities that may not have been foreseen.

IV. WEAPONS REVIEWS OF CYBER WEAPONS

The determination that certain cyber capabilities constitute weapons leads to the inescapable conclusion that they require legal review. While all States are legally obliged, as a matter of customary law, to "ensure that the means of cyber warfare that they acquire or use comply with the rules of the law of armed conflict,"[47] Article 36 of AP I requires that

> in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[48]

The customary law obligation to review new weapons follows from the general obligation of States to comply with their weapons law duties.[49]

Of the relatively few States that are known to have systems for such review, the UK and U.S. systems, and those in Belgium, Canada, Australia, the Netherlands, Norway, France and Sweden, take the form of a generic

47. TALLINN MANUAL, *supra* note 9, rule 48(a).

48. Rule 48(b) of the *Tallinn Manual* applies this treaty rule specifically to cyber means and methods of warfare.

49. Consider the liability, in appropriate circumstances, to pay compensation in the event of violations of the law of armed conflict in Article 3 of Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2227 and Article 91 of Additional Protocol I. Consider also International Committee of the Red Cross, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare, Measures to Implement Article 36 of Additional Protocol I of 1977*, 88 INTERNATIONAL REVIEW OF THE RED CROSS 931, 935 (2006) [hereinafter ICRC Guide]; W. Hays Parks, *Conventional Weapons and Weapons Reviews*, 8 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 55, 57 n.6 (2005). The customary law prohibition of weapons of a nature to cause superfluous injury or unnecessary suffering seems to imply an obligation to assess new weapons by reference to that standard.

review of the weapon in the light of its intended circumstances of use. The review is undertaken before the weapon is released to the armed forces for use in armed conflict.[50] The AP I, Article 82[51] targeting advice to commanders that is provided ad hoc with regard to planned attacks is generally regarded as distinct from the weapon review. Thus, before a non-cyber weapon has been released to the armed forces for employment in combat, commanders will know that it has been the subject of legal review and that the designed or intended use of it, as determined at the time of procurement, accords with the State's international law obligations.

There are, however, characteristics peculiar to cyber weapons that will make the giving of weapons law advice at the development or procurement stage difficult to achieve. A cyber weapon may at that point be so generic in nature that the giving of any meaningful advice as to its compliance with international law becomes speculative. The very nature of the weapon as discriminate or otherwise, and the nature and extent of the generic injury and suffering it will cause, may fundamentally depend on the nature, linkages, dependencies and customer base of the target computer system. In such circumstances, realistic weapons law advice can only be given when those variables are known. This has two obvious consequences. The first is that the operational commander contemplating use of such a weapon may not know in advance that the weapon will be lawful in the circumstances of the use that he intends. The second, consequent on the first, is that the lawyer fulfilling the Article 82 duty to advise a commander with respect to a planned cyber attack may need to build both weapons law and targeting law aspects into his legal advice to the commander.

The weapons law part of such ad hoc advice to the commander will therefore need to consider the context of the attack; the first, second and third order effects that the weapon is expected to produce; the collateral damage expected to civilian users of the target computer system; and whether the nature of the cyber weapon is such as to enable the injury or damage to be restricted to the military objective. In such circumstances, it is obvious that the weapons law advice and the targeting law advice will tend to merge. Even the weapons law assessment of whether the weapon is

50. *See* ICRC Guide, *supra* note 49, at 934.

51. The High Contracting Parties at all times, and the Parties to the conflict in time of armed conflict, shall ensure that legal advisers are available, when necessary, to advise military commanders at the appropriate level on the application of the Conventions and [the] Protocol and on the appropriate instruction to be given to the armed forces on this subject.

capable of being used discriminately and in compliance with the superfluous injury/unnecessary suffering principle will be eclipsed by the issue of whether the planned attack, taking into account the cyber weapon to be used, the circumstances of the target system and of any other nodes liable to be affected, will comply with the customary law targeting rules, and for States party to AP I, with Articles 48 to 67. While this is appreciated, nevertheless, the ad hoc weapons law issues discussed in this article must also be considered, if only to conclude that they have no relevance to the particular circumstances.

Perhaps the safest way forward is for a legal review of all cyber weapons to continue to be undertaken at the weapon development stage. Such reviews can be used to inform the concept of use and associated documents in which the requirement for ad hoc weapons law advice concerning particular types of attack can be noted. Advisers to commanders must, however, appreciate that when advising on planned cyber attacks, a wider range of issues will need to be considered for the reasons set out earlier.

V. APPLYING WEAPONS LAW TO PARTICULAR TYPES OF CYBER WEAPONS

Consideration will now be given to how the weapons law previously discussed can be applied to particular kinds of cyber tools. For these purposes, on an illustrative basis, the use of botnets to deny the services of a targeted computer system, the planting of a kill switch and masquerade will be examined.

Malware might be used to take control of a number of infected computers that become a virtual network centrally controlled by command and control servers. Spam messages are then, for example, sent to the targeted computer system, the bandwidth of which is exhausted, thus prompting the denial-of-service from the targeted system that was the goal of the cyber operation. The malware will cause resources of the infected computers in the net, or bots as they are known, to be devoted to the operation so services to the customers of those systems may also be affected. However, the denial or deterioration of service will only last as long as the botnet is operated and there will normally be no lasting effect on the targeted system. The effect on the targeted computer system will not, therefore, amount to "damage" such that the botnet tool will not thereby be rendered a weapon. If, however, as an example, the targeted system provides life support services that when interrupted will foreseeably cause death or injury, such a use of the cyber tool would render it a weapon requiring legal review.

In conducting that review, the rules of weapons law discussed in this article should be applied. The nature and degree of the injuries suffered and to be expected as a result of such a cyber attack will determine whether the superfluous injury/unnecessary suffering rule has been complied with. More problematic may be the prohibition of cyber weapons that are indiscriminate by nature. It is, however, only death, injury, damage or destruction to protected persons or objects that should be considered. Inconvenience or annoyance caused, for example, by collateral denials-of-service from computer systems forming the botnet will not cause the cyber tool to be indiscriminate by nature.

The use of a targeted Trojan to plant a kill switch involves sending customized—typically concealed—malware to an unaware individual. That individual, by running an apparently safe program or computer file, unknowingly infects the receiving computer system with malware comprising a kill switch. The malware enables the cyber attacker to take control of the target computer system giving him access to all the data stored there. The kill switch can, for example, disable operating programs, corrupt data or close down the target computer system either in response to a command from the cyber attacker or when the authorized operator performs some routine operation, such as switching on the computer. When reviewing such a cyber tool under weapons law, the superfluous injury/unnecessary suffering rule will only need to be considered if the cyber tool, in its intended circumstances of use, is designed or intended to cause injury or death. In deciding whether, when used as intended, the cyber tool is indiscriminate by nature, the designed or intended consequences of activating the kill switch will be critical. Similar considerations to those discussed in the previous paragraph will arise. If the kill switch is designed or adapted to cause death or injury, legal reviewers from states that are party to Protocol II and/or Amended Protocol II to the CCW will consider whether, according to their State's interpretation, such a device amounts to a booby-trap for the purposes of those treaties. Similarly, if the malware containing the kill switch is to be applied to the target computer manually, for example by means of a thumb drive, and if the device is designed to kill, to cause injury or to damage property, the legal reviewer should consider his State's understanding of the definition of "other device" in Protocol II and Amended Protocol II.[52] If the kill switch is to be actuated by remote control, for ex-

52. CCW Protocol II *supra* note 38, art. 2(3) and CCW Amended Protocol II, *supra* note 38, art. 2(5).

ample by a command from the cyber attacker, or if it will activate automatically after a specified time period has elapsed, then the requirements of both Protocols concerning "other devices" will potentially apply to the cyber weapon. If the kill switch is designed to be actuated by a manual act, the provisions of Amended Protocol II relating to "other devices" will potentially apply to the weapon. Here again, much will depend on the relevant State's interpretation of the word "manually." The author considers that, when considered in the context of the Protocols as a whole, "manually" implies a degree of physical connection between the actor and the device which is likely to be absent in the stated example. This is because, in the example, the physical connection is between the actor and the thumb drive, not the device as such.

Masquerade, as a cyber operation, involves the creation of a computer system that mimics the targeted computer system. Customers of the targeted system are diverted to the masquerade system or site where the visiting computer may be infected or where deliberately wrong messages may be given. Clearly, such a cyber tool can be used for a variety of deception-based operations, some of which would be unlawful.[53] Cyber capabilities used for deception-based operations that do not result in death, injury, damage or destruction do not, however, constitute weapons, means or methods of warfare. It is only, therefore, when the masquerade operation is designed or intended to cause death, injury or damage that the cyber tool becomes a cyber weapon requiring legal review. The legal principles prohibiting weapons of a nature to cause superfluous injury/unnecessary suffering or to be indiscriminate will then apply to the masquerade operation. Thus, for example, if the lethal, injurious or damaging effects of the malware cannot be controlled or limited reasonably to military objectives, the cyber weapon is liable to be considered indiscriminate by nature.

53. Consider, for example, the AP I prohibition on causing death, injury or capture by resort to perfidy (Article 37), the prohibition on making improper use of the distinctive emblems (Article 38(1)), the prohibition of unauthorized use of the United Nations emblem (Article 38(2)), the prohibition on using flags, emblems or insignia of neutrals (Article 39(1)) and the prohibition on using flags, military emblems, insignia or uniforms of adverse parties during attacks or in order to shield, favor, protect or impede military operations (Article 39(2)).

VI. CONCLUDING REMARKS

As these illustrations demonstrate, distinctions between the law of weaponry and the law of targeting that have considerable logic when applied to traditional kinetic weapons are more difficult to maintain in the cyber context. As an example, the generic cyber capability of using a targeted Trojan to plant a kill switch may breach the rule prohibiting indiscriminate weapons—or it may not. Much will depend (i) on the nature and characteristics of the chosen targeted computer system; (ii) the customers of the target system; (iii) on whether those customers are liable further to spread the malware—innocently or otherwise; (iv) on whether the kill switch when used against the intended target is designed to cause death, injury or damage; and (v) on numerous other features peculiar to the specific intended cyber operation.

Accordingly, a weapon review of such a generic capability should consider the likely applications of the cyber tool, taking into account what the tool is designed to do and how it is designed to do it. The review should discuss which potential applications, if any, would breach the weapons law rules applicable to that State and should identify whether there are restrictions on the lawful use of the cyber tool. It will then be for the legal adviser to the operational commander to consider the intended cyber operation by reference to both weapons law and targeting law norms.

It is evident from the analysis in this article that a useful focus for future research and cyber weapons development would be to enhance the ability of a cyber attacker to control and limit the effects of cyber weapons. This implies the need to be able to direct the weapon at the intended target, to limit its effects to that target and to be able to switch off the damaging operations if it ceases to operate as intended. Cyber weapons that lack any of these features will not necessarily be unlawful; however, enhancing the ability to control—possibly even to reverse—cyber effects would seem to be a future, if not a present, priority given ever increasing cyber dependence.