Federal Communications Law Journal

Volume 64 | Issue 3 Article 8

5-2012

Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?

Anna Wortham
Indiana University School of Law

Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?

Anna Wortham*

I. INTRODUCTION 644
II. CYBER ATTACK AND CYBER EXPLOITATION 646
A. *Difference Between Cyber Attacks and Cyber Exploitations Generally* 646
B. *Comparison of Cyber Attacks and Cyber Exploitations* .. 646
III. LOAC AND THE UN CHARTER 647
A. *Laws That Apply to Cyber Attack and Cyber Exploitation Generally* 647
B. *The Law of Armed Conflict* 647
1. *Jus Ad Bellum* and *Jus In Bello* 647
2. Specific Laws Governing *Jus Ad Bellum* 648
IV. DIFFICULTIES APPLYING LOAC AND UN CHARTER PROVISIONS 650

* J.D. Candidate, Indiana University Maurer School of Law, May 2013; B.A. in English, Brigham Young University, April 2010. The Author would like to thank the members of the *Federal Communications Law Journal* for their help preparing this Note for publication. In addition, the Author would like to thank her husband for believing in her and her parents for constantly encouraging her to do her best.

A. Physical Injury and Destruction vs. Infrastructure Controlled by Technology 650
B. Cyber Attack Weapons Are Readily Available, Not Just Available to Governments 651
C. Presumption of Nation-to-Nation Conflict Between National Military Forces 651
D. The Interconnection of Military and Civilian Information Technology 651
E. The Exception for Espionage 652
F. The Problem of Attribution 653
V. CYBER EXPLOITATION AS A THREAT OR USE OF FORCE 655
A. Cyber Exploitation as a "Use of Force" Under Current Laws 655
B. Cyber Exploitation as a Threat of Force Under Current Laws 655
C. Cyber Exploitation and Anticipatory Self-Defense Under Current Laws 656
VI. NEW LAWS FOR CYBER THREATS: CYBER EXPLOITATION AS ESPIONAGE? 657
A. Espionage Generally 657
B. Differences Between Cyber Exploitation and Traditional Espionage 658
1. Access to Much Larger Breadth of Material 658
2. Much Easier and Less Expensive Access 659
3. Unknown Effects, Spread to Unintended Targets 659
4. Attribution Is Near Impossible 659
5. Long Time to Investigate, Few Conclusive Answers .. 660
VII. CONCLUSION 660

I. INTRODUCTION

As the United States and other countries rely more and more on complex infrastructures that are primarily controlled by information technology, and cyber threats against nations become a reality, clear international laws on cyber threats become a necessity. In light of the fact that the United States and other nations may use cyber capabilities offensively as well as defensively, it is even more important that the laws for engaging in such cyber conflict are clear. This is especially true in the case of cyber exploitation because the effects of such exploitations can be far-reaching, but the international law regarding these exploitations is far from clear. Currently, it seems unlikely that cyber exploitation can ever be

regarded as a threat or use of force under the UN Charter because it is typically regarded as espionage, which is permissible internationally.

This Note first analyzes whether it is the case that cyber exploitation cannot constitute a threat or use of force and then analyzes whether that should be the case. Section II focuses on cyber attack and cyber exploitation generally, explaining the differences between the two threats and the similarities in the ways the two threats are carried out. Section III discusses what body of law is applicable to cyber attack and cyber exploitation when a nation engages in or defends against one of these threats, specifically the Laws of Armed Conflict ("LOAC") and the UN Charter. Section IV discusses some of the primary difficulties in applying LOAC and the UN Charter to cyber threats. Section V analyzes whether cyber exploitation, under current governing law, can ever constitute a use of force, constitute a threat of force, or justify anticipatory self-defense. This section concludes that cyber exploitation, by itself, likely cannot constitute a threat or use of force under current law. Section VI then analyzes whether cyber exploitation should continue to be treated similar to traditional espionage in the international setting, which would result in it never being considered a threat or use of force. This section argues that cyber exploitation should be treated differently than traditional espionage and lays out several reasons why this should be the case. Ultimately, this Note concludes that because cyber exploitation is so different from traditional espionage, cyber exploitation should be able to constitute a threat or use of force by itself in some cases. In situations where it does not rise to the level of threat or use of force, it should still be prohibited internationally because it can be so much more destructive than traditional espionage.

While this Note primarily focuses on the questions surrounding cyber exploitation, the similarities between cyber attack and cyber exploitation make the discussion of cyber attack in this paper requisite. Because there has not been much written on the subject of cyber exploitation or cyber attacks and how they should be dealt with in an international "armed conflict" sense, the majority of the background information in this Note is founded on information presented in the 2009 National Research Council Report ("*NRC Report*").[1]

---

1. NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) [hereinafter NRC REPORT].

II. CYBER ATTACK AND CYBER EXPLOITATION

A. Difference Between Cyber Attacks and Cyber Exploitations Generally

Cyber attacks and cyber exploitations are the two forms of hostile actions that may be taken against a computer system or network.[2] While many people lump these two categories together under the title of cyber attacks, cyber attack and cyber exploitation are two distinct actions. According to the *NRC Report*, "[c]yber attack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[3] The purpose of a cyber attack is to make adversary computer systems and networks less useful to the adversary by making them unavailable or untrustworthy.[4] Cyber exploitation, on the other hand, refers to "the use of cyber offensive actions . . . usually for the purpose of obtaining information resident on or transiting through an adversary's computer systems or networks."[5] The main difference between cyber attack and cyber exploitation is that cyber attack is destructive in nature while cyber exploitation is focused on intelligence gathering and, in order to be covert, purposely does not try to affect the normal processes of the computer or network exploited.

B. Comparison of Cyber Attacks and Cyber Exploitations

With regard to operational considerations, cyber exploitation and cyber attack are very similar. Both cyber attack and cyber exploitation require a vulnerability, access to the vulnerability, and a payload to be executed.[6] The payload to be executed, though, differs between the two. Cyber exploitation requires that the execution of the payload be accomplished clandestinely, while secrecy is often far less important with

---

2. Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63, 63 (2010).

3. NRC REPORT, *supra* note 1. The *NRC Report* states that "[a]n adversary computer or network may not necessarily be owned and operated by the adversary—it may simply support or be used by the adversary." *Id.* at 11 n.4.

4. *Id.* at 11.

5. *Id.*

6. *Id.* at 20 ("For a computer or network, a vulnerability is an aspect of the system that can be used by the attacker to compromise [the system] . . . ."). Vulnerabilities can be introduced either intentionally or accidentally. *Id.* at 83. "Payload is the term used to describe the things that can be done once a vulnerability has been exploited." *Id.* at 88.

cyber attacks because the effects of the cyber attack are often readily apparent to the target.[7]

The process of intelligence gathering necessary to penetrate an adversary's computer or network is almost identical for both cyber exploitation and cyber attack.[8] Both cyber attack and cyber exploitation use the same kind of access paths to reach their targets and also "take advantage of the same vulnerabilities to deliver their payloads."[9] Because of the aforementioned similarities, an adversary's intent is often extremely difficult, if not impossible, to determine.[10] This topic will be revisited later in this Note.

III. LOAC AND THE UN CHARTER

A. Laws That Apply to Cyber Attack and Cyber Exploitation Generally

The rules that apply when a nation engages in or defends against a cyber attack or cyber exploitation are not entirely clear. Although cyber-specific rules have been created in many instances for cybercrime, nations have not created cyber-specific rules for the actions they take against other nations.[11] Therefore, most international laws have to be applied by analogy. The main body of relevant international laws, and the body of laws most pertinent for the discussion of this Note, is the LOAC.

B. The Law of Armed Conflict

1. *Jus Ad Bellum* and *Jus In Bello*

LOAC addresses two questions: (1) "[W]hen is it legal for a nation to use force against another nation?" and (2) "[W]hat are the rules that govern the behavior of combatants who are engaged in armed conflict?"[12] The law governing when a nation can use force against another nation is known as *jus ad bellum*.[13] *Jus ad bellum* refers to "those established 'conflict management' norms and procedures that dictate when a state may—and

7. *Id.* at 20–21.
8. *Id.* at 155.
9. *Id.*
10. *Id.*
11. Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 393 (2011).
12. NRC REPORT, *supra* note 1, at 242.
13. *Id.*

may not—legitimately use force as an instrument of dispute resolution."[14] The law governing when nations are involved in armed conflict, which is separate and distinct from *jus ad bellum*, is known as *jus in bello*.[15] Because this Note focuses on whether or not cyber exploitations can ever constitute a "threat or use of force" that would permit a targeted nation to retaliate*, jus ad bellum* is the relevant body of law.

2. Specific Laws Governing *Jus Ad Bellum*

According to the *NRC Report*, "[j]us ad bellum is governed by the UN Charter, interpretations of the UN Charter, and some customary international law that has developed in connection with and sometimes prior to the UN Charter."[16] *Jus ad bellum* and the UN Charter specifically apply to covert action such as cyber exploitation.[17] The UN Charter provisions most applicable to *jus ad bellum* are Articles 2(4), 39, 41, 42, and 51.[18]

The aforementioned articles of the UN Charter lay out the basic framework of *jus ad bellum*. Article 2(4) sets forth the prohibition against the threat or use of force.[19] Specifically, Article 2(4) prohibits every nation from using "the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[20] Professor Wingfield of the U.S. Army Command and General Staff College testified to the committee putting together the *NRC Report* that some threats that might constitute "threats of force" according to Article 2(4) include "verbal threats, initial troop movements, initial movement of ballistic missiles, massing of troops on a border, use of fire control radars, and interference with early warning or command and control systems."[21]

Articles 39, 41, and 42 define the Security Council's authority. Article 39 gives the Security Council the authority to "determine the existence of any threat to the peace, breach of the peace, or act of aggression and [to] make recommendations, or decide what measures shall be taken in

---

14. David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87 (2010) (citing John Norton Moore, NATIONAL SECURITY LAW 29 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005).

15. NRC REPORT, *supra* note 1, at 242.

16. *Id.* (emphasis omitted).

17. *Id.*

18. *See* Graham, *supra* note 14, at 88; Lin, *supra* note 2, at 71; NRC REPORT, *supra* note 1, at 257.

19. U.N. Charter art. 2, para. 4.

20. *Id.*

21. NRC REPORT, *supra* note 1, at 242.

accordance with Articles 41 and 42, to maintain or restore international peace and security."[22] In Article 41, the Security Council is given the authority to "decide what measures not involving the use of armed force are to be employed to give effect to its decisions . . . ."[23] In Article 42, the Security Council is given the authority to take "such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security" if it decides "measures provided for in Article 41 would be inadequate or have proved to be inadequate . . . ."[24]

Despite all the aforementioned provisions of the UN Charter, Article 51 states that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[25] Article 51 provides an exception to the absolute prohibition against the use of force put forth in Article 2(4), permitting nations to use force out of self-defense. Whether Article 51 recognizes a pre-existent right to self-defense or limits that right of self-defense is presently being debated.[26]

The only other exception to the absolute prohibition against the use of force is that set forth in Article 39, which states that nations are allowed to use force if given permission by the Security Council.[27] Articles 39 and 42, together, allow the Security Council to authorize uses of force.[28] An important note is that a nation does not need Security Council permission in order to act in self-defense as permitted by Article 51.[29]

In some instances, nations are allowed to act out of "anticipatory self-defense" before an attack has even been launched.[30] Although this right is not explicitly stated in Article 51, when a nation is facing an unambiguous attack, it is widely accepted that the interpretation of Article 51 allows a nation to act out of self-defense prior to the attack.[31] This right of anticipatory self-defense is explained in *Oppenheim's International Law*, where it states:

> [T]he use of armed force and the violation of another state's territory, can be justified as self-defence under international law where: (a) an

22. U.N. Charter art. 39.
23. *Id.* at art. 41.
24. *Id.* at art. 42.
25. *Id.* at art. 51.
26. NRC REPORT, *supra* note 1, at 243.
27. Graham, *supra* note 14, at 88; U.N. Charter arts. 39, 51.
28. U.N. Charter arts. 39, 42; Lin, *supra* note 2, at 71.
29. NRC REPORT, *supra* note 1, at 243. *See* U.N. Charter art. 51.
30. NRC REPORT, *supra* note 1, at 243.
31. U.N. Charter art. 51; NRC REPORT, *supra* note 1, at 243.

> armed attack is launched, or is immediately threatened, against a state's territory or forces . . . (b) there is an urgent necessity for defensive action against that attack; (c) there is no practicable alternative to action in self-defence, . . . [and] (d) the action taken by way of self-defence is limited to what is necessary to stop or prevent the infringement . . . .[32]

When a nation can use anticipatory self-defense, though, is not clear. Often, the "threatened party is likely to have a rather different perception of such facts and circumstances than the threatening state."[33] The *NRC Report* explains:

> The mere fact that Zendia possesses destructive capabilities that could be used against Ruritania cannot be sufficient to indicate imminent attack—otherwise, the mere existence of armed forces of an adversary would be sufficient justification. But if Zendia can use these capabilities effectively against Ruritania and with serious consequences without warning, and Zendia has indicated hostile intent toward Ruritania in other (perhaps nonmilitary) ways, outside observers may indeed be more likely to judge that the conditions for anticipatory self-defense have been met.[34]

IV. DIFFICULTIES APPLYING LOAC AND UN CHARTER PROVISIONS

What specifically counts as a threat or use of force under Article 2(4) in a cyber context? Because of the technology used in cyber attacks and cyber exploitations, it is very difficult to actually apply LOAC and UN Charter provisions. Oftentimes, the only way to apply LOAC and UN Charter provisions is through analogy. Below, this Note discusses some of the main reasons that applying LOAC and UN Charter provisions to cyber attacks and cyber exploitations is difficult.

A. Physical Injury and Destruction vs. Infrastructure Controlled by Technology

Much of society today relies on an infrastructure that is controlled in large part by information technology. Interference with that infrastructure, regardless of whether physical damage is caused, can constitute an armed attack under Article 51.[35] In order to determine if a cyber attack or exploitation should constitute a threat or use of force, the effects of the attack or exploitation are the most important aspect of the threats to

---

32. 1 OPPENHEIM'S INTERNATIONAL LAW 422 (Robert Jennings & Arthur Watts eds., 9th ed. 1992).

33. NRC REPORT, *supra* note 1, at 243.

34. *Id.* at 243, 246.

35. *Id.* at 254.

analyze.[36] If the effects produced by a cyber threat would constitute a use of force if produced by other means under LOAC and the UN Charter, then the threat will likely constitute a use of force.[37] The opposite is also true.[38]

B. Cyber Attack Weapons Are Readily Available, Not Just Available to Governments

The technology needed to launch a cyber attack or exploitation is widely available today. Nonstate actors can launch cyber attacks and exploitations quite easily and can often do just as much harm as state actors.[39] The inability to know whether an actor is a state actor or not makes applying LOAC and the UN Charter difficult because these laws are built upon the presumption that it is clear when LOAC should be applied and when national criminal laws should be applied.[40]

C. Presumption of Nation-to-Nation Conflict Between National Military Forces

Closely related to the last difficulty discussed, LOAC and UN Charter provisions assume that the actors are nations and that national military forces are involved in the conflict.[41] LOAC and UN Charter provisions are much harder to apply when nonstate actors must be taken into consideration.[42]

D. The Interconnection of Military and Civilian Information Technology

Furthermore, today military and civilian information technology is interconnected.[43] The "LOAC and UN Charter [are] based on the idea that civilian and military assets can be separated . . . ."[44] Because this is not the case in the cyber realm, directly applying LOAC and UN Charter provisions is extremely difficult.

---

36. *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999); Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57 (2001).

37. NRC REPORT, *supra* note 1, at 272.

38. *Id.*

39. *Id.* at 22.

40. *Id.*

41. *Id*. at 273.

42. *Id*. at 273–74.

43. *Id.* at 35.

44. *Id.*

E. The Exception for Espionage

The LOAC also assumes that espionage and the use of force are two distinct actions.[45] In the cyber realm, however, this is often not the case. This is an incredibly important point because espionage and uses of force are treated very differently. Espionage is not deemed an illegal activity under international law,[46] as "there are no treaties or customary norms that explicitly proscribe the practice."[47] According to Hays Parks:

> Each nation endeavors to deny intelligence gathering within its territory through domestic laws . . . . Prosecution under domestic law (or the threat thereof) constitutes a form of denial of information rather than the assertion of a *per se* violation of international law; domestic laws are promulgated in such a way as to deny foreign intelligence collection efforts within a nation's territory without inhibiting that nation's efforts to collect intelligence about other nations. No serious proposal has ever been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgement by nations that it is important to all, and practiced by each.[48]

Nations seem to agree that espionage, among other activities, is not enough to count as a use of force.[49] And many nations recognize cyber exploitation as a new method of espionage.[50] As stated in the *NRC Report*, if the legal approach set forth by Hays Parks is accepted, cyber exploitations, which are generally thought of as espionage conducted through a computer, would be permissible under LOAC.[51] And this could be the case even if the cyber exploitation is conducted in a manner that could also aid a destructive cyber attack.[52]

Because there are so many similarities between cyber attack and cyber exploitation, it is often difficult to determine whether a party has been exploited or attacked.[53] Vulnerabilities in many cases can be used for either cyber attack, cyber exploitation, or both.[54] While cyber exploitations

---

45. *Id.* at 22.

46. *Id.* at 259.

47. Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162, 1165 (2011).

48. Lin, *supra* note 2, at 72 (quoting W. Hays Parks, *The International Law of Intelligence Collection*, in NATIONAL SECURITY LAW 433, 433–34 (John Norton Moore et al. eds., 1990)).

49. NRC REPORT, *supra* note 1, at 242.

50. Hollis, *supra* note 11, at 395. *See* Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1072 (2006).

51. NRC REPORT, *supra* note 1, at 261.

52. *Id.*

53. *Id.*

54. Hollis, *supra* note 11, at 386.

are not typically considered capable of being deemed a use of force, their similarities to cyber attacks often make it difficult to tell the two types of actions apart.

Even when an action is limited exclusively to cyber exploitation, the potential to use that same vulnerability for a later cyber attack is still present.[55] So when do these actions in the cyber context cross the line and count as threats or uses of force? If someone threatens to use an existing vulnerability in an adversary computer system or network, does that constitute a threat of force under the UN Charter?[56] What about simply introducing vulnerabilities into an adversary's system or network?[57] Do those vulnerabilities have to be used within a certain time period for the threat to be real? Does there have to be evidence of an imminent attack or use of the vulnerability first before it can constitute a threat of force? Does finding a vulnerability alone justify using anticipatory self-defense? These are just some of the questions that analysts and policy makers are confronted with in the cyber realm.

Furthermore, the cost to equip a cyber exploitation with the capability of a later cyber attack is extremely low, and it often makes sense to add such capabilities, whether or not those capabilities will ever be realized.[58] Because of the ease with which a cyber exploitation can be outfitted to conduct a cyber attack and the fact that these two cyber threats do not have to be mutually exclusive, a targeted party oftentimes will not know, and will have no way of finding out, whether it has been attacked, exploited, or both. This problem is further compounded because of the time constraints that often exist when dealing with and making decisions regarding such national threats.[59]

F. The Problem of Attribution

Discussed briefly above, another difficulty in applying LOAC and the UN Charter stems from the problem of attribution inherent to cyber technology. Attribution refers to "the ability to identify the party responsible for an offensive cyber operation based only on technical indicators and information associated with that operation."[60] Both the

---

55. *Id.*

56. NRC REPORT, *supra* note 1, at 257.

57. *Id.*

58. *Id.* at 152 n.60 ("If these [cyber exploitation] tools were to be used against U.S. citizens . . . legal and/or policy implications might arise if these tools were to have attack capabilities as well. Thus, the observation is most likely to be true for tools that are not intended for such use.").

59. *Id.* at 273.

60. Lin, *supra* note 2, at 77.

LOAC and UN Charter assume that nations are necessarily involved and that those nations are either known or identifiable.[61] However, the very makeup of the Internet makes attribution in many cases nearly impossible.[62] While some level of attribution can be attained by acquiring information from nontechnical sources, such as human intelligence, it is often difficult to ascertain "when an offensive cyber operation has begun, who the attacker is, and what the operation's purpose and effects are or were."[63] And in many cases with cyber attacks and cyber exploitations, the actor is never discovered. For example, the authors of the 2007 Estonia attacks, the 2008 Georgian attacks, the July 4, 2009 attacks, and the implanting of logic bombs in the U.S. power grid are still largely unknown.[64]

The problem of attribution leads to many offshoot difficulties. One of those difficulties resulting from the problem of attribution is the issue of geography. When a nation has been the target of a cyber attack or exploitation, is it the computer's physical location that is relevant when the nation is trying to determine what to attack in response, or is it some other geographic location?[65]

Another difficulty resulting from the problem of attribution is knowing how to treat the action—should it be treated as a crime or an act of war?[66] If the actor is a nation, then the problem should be treated as a national security issue rather than a law enforcement case.[67] If the actor is misunderstood or misidentified, the wrong set of rules could easily be applied, though, and this could lead to the use of military force.[68]

However, not knowing the actor does not mean that defensive actions are prohibited. According to the U.S. Defense Department, international law does not require that an actor must be known before defensive action can be taken.[69] Rather, the responsibility for the attack would be imputed "to the state to whose territory the attack was traced."[70]

---

61. *See* NRC REPORT, *supra* note 1, at 293–94.

62. David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 323, 345–46 (2011).

63. Lin, *supra* note 2, at 77.

64. Hollis, *supra* note 11, at 405.

65. *See* NRC REPORT, *supra* note 1, at 36.

66. Hollis, *supra* note 11, at 405.

67. Clark & Landau, *supra* note 62, at 345.

68. Hollis, *supra* note 11, at 405.

69. *Id.* at 406.

70. *Id.*

V. CYBER EXPLOITATION AS A THREAT OR USE OF FORCE

Given the issues previously discussed, can cyber exploitation ever constitute a "threat or use of force" under LOAC and the UN Charter?

A. Cyber Exploitation as a "Use of Force" Under Current Laws

Under the current legal structure, cyber exploitation by itself seems to clearly never constitute a use of force. As stated above, most countries consider cyber exploitation a new form of espionage, and espionage traditionally does not constitute a use of force. While a cyber attack can constitute a use of force if the effects are such that they traditionally would have been achieved through a kinetic attack, cyber exploitation is regarded differently.

However, as shown through the explanation of some of the difficulties in applying LOAC and UN Charter provisions to the cyber realm and the discussion of the similarities between cyber attack and exploitation, the distinctions between cyber attack and exploitation are not always clear. Because of the similarities between cyber attack and exploitation, targeted nations will typically not know what kind of cyber threat with which they are faced. When time constraints in responding to national threats are subsequently added to the already uncertain situation, it is easy to envision a nation misinterpreting a cyber threat and responding in a manner that would escalate the situation to armed conflict when in fact the situation had started out as a cyber exploitation.

B. Cyber Exploitation as a Threat of Force Under Current Laws

While it seems pretty clear from the few articles and reports written on the subject that an isolated cyber exploitation will never by itself constitute a *use* of force, there is very little written on the question of whether a cyber exploitation can ever constitute a *threat* of force.[71] Like a use of force, it would seem that the detection of an isolated cyber exploitation would also never constitute a threat of force for the same reasons. Traditionally, espionage simply cannot justify retaliation in the form of armed conflict.[72] However, it is under the category of threat of force that there is much more ambiguity; the bar is lower in order for something to qualify as a threat of force.[73] In order for a risk to constitute a "threat" of force, it is not requisite that there be any physical harm or readily evident destruction. There simply has to be a threat.

---

71. *See generally* NRC REPORT, *supra* note 1.
72. *Espionage*, in 4 WEST'S ENCYCLOPEDIA OF AMERICAN LAW 299 (1998).
73. *See* NRC REPORT, *supra* note 1, at 257.

Because the same vulnerabilities can be used to perpetrate an attack, an exploitation, or both, if a nation identifies a vulnerability in a computer network that has been taken advantage of (or even simply that a vulnerability has been accessed in a manner that it can be taken advantage of easily at a later date), there is practically no way for that nation to tell what the intent of the attacking party was or is. When does identifying a vulnerability become a threat of force? Do some initial steps have to be taken to actually use the accessed vulnerability for a future attack? What if the vulnerability has already been taken advantage of for exploitation purposes over time? Can simply identifying the exploitation of information then constitute a "threat" of force because there is the potential to use the same vulnerability at a later time to initiate an attack? While it is not likely that simply identifying a vulnerability that has been used for intelligence collection would ever constitute a threat of force on its own, perhaps the combination of an identified vulnerability and other intelligence information that shows the likelihood of a future attack would be able to constitute a threat of force.

C. Cyber Exploitation and Anticipatory Self-Defense Under Current Laws

Similar to the question of whether cyber exploitation can ever constitute a *threat* of force is the question of whether a nation can ever act out of anticipatory self-defense because of cyber exploitation. While, as with the two previous sections, cyber exploitation by itself seems like it would never justify a targeted nation's use of anticipatory self-defense, the threat of cyber attack that is posed by the vulnerabilities accessed in cyber exploitation might in some cases justify its use.

As explained in *Oppenheim's International Law*, the factors that must be present in order for anticipatory self-defense to be appropriate are: (1) the immediate threat of attack; (2) the urgent necessity to defensively act against the attack; and (3) that no practicable alternative to self-defense exists.[74] Furthermore, it is requisite that the act of self-defense is appropriately limited in scope to that which is necessary to prevent the infringement.[75] Because of the requirement that the threat of attack be immediate,[76] simply recognizing an accessed vulnerability would not seem to be enough to justify the use of anticipatory self-defense. Under this legal regime, the only instance in which cyber exploitation would appear to ever justify anticipatory self-defense is in the case where both (1) a cyber

74. OPPENHEIM'S INTERNATIONAL LAW, *supra* note 32, at 422.
75. *Id.*
76. *Id*.

exploitation vulnerability that can be used at a future date is located and (2) where intelligence information that the particular vulnerability will in fact be used for an imminent attack has been obtained.

VI. NEW LAWS FOR CYBER THREATS: CYBER EXPLOITATION AS ESPIONAGE?

In order to account for cyber threats, specifically cyber exploitation and its ability to easily lend itself to cyber attack, there needs to be a new or amended set of international laws. If the same legal regime continues to be used, the consequences could be dire.

Many of the considerations that the new laws should take into account are the difficulties discussed previously with applying LOAC and the UN Charter to cyber threats: the new governing laws need to take into consideration that today's society is heavily reliant on an infrastructure that is controlled by information technology, that cyber weapons are easily available and can easily be used by nonstate actors, that conflict is not just between nations and national military forces anymore, that military and civilian sectors are interconnected and share information technology, that cyber exploitation is different from traditional espionage, and that the actors of cyber attacks often cannot be identified.

The rest of this Note is primarily discusses how cyber exploitation should be treated differently than traditional espionage. The capabilities of cyber technology simply differ too much from those of traditional espionage, and the ease with which the technologies for cyber exploitation and cyber attack can be used together demands a new set of laws.

A. Espionage Generally

According to *West's Encyclopedia of American Law*, espionage is "[t]he act of securing information of a military or political nature that a competing nation holds secret," and it is "commonly known as spying . . . ."[77] As stated previously, federal criminal laws prohibit the practice of espionage,[78] but it is a generally accepted activity in the international community.[79]

77. WEST'S ENCYCLOPEDIA OF AMERICAN LAW, *supra* note 72, at 299.
78. 18 U.S.C. § 793 (2006).
79. WEST'S ENCYCLOPEDIA OF AMERICAN LAW, *supra* note 72, at 299.

B. Differences Between Cyber Exploitation and Traditional Espionage

While cyber exploitation falls within the above definition of espionage, as it is a means of obtaining secret national information, cyber exploitation does not fit the traditional understanding of espionage, where nations send attachés and spies in order to gather intelligence information.[80] Because cyber exploitation is so much more intrusive than traditional espionage and can be conducted effectively by nonstate actors in ways that can undermine a targeted nation's infrastructure or launch an attack on another nation, it needs to be treated as a higher concern than traditional espionage. A 2009 investigation into a series of Chinese cyber exploitations targeted at Tibet is an example of some of the differences between cyber exploitation and what this Note refers to as traditional espionage.[81]

The Information Warfare Monitor conducted an in-depth investigation of cyber exploitation against the Tibetan community, which was allegedly carried out by China.[82] The exploitation was carried out by a "malware-based cyber espionage network" referred to as *GhostNet*.[83] The *GhostNet* system directed infected computers to download a Trojan, *gh0st RAT*.[84] Once downloaded, exploiters gained complete, real-time control of the computer, allowing them to search and download files, as well as covertly operate attached devices such as microphones and web cameras.[85]

1. Access to Much Larger Breadth of Material

One reason cyber exploitation should be treated differently than traditional espionage is because of the greater breadth of material that cyber exploitation can provide access to. The more knowledge about a foreign nation that can be obtained, the more dangerous that information can become. In the case of *GhostNet*, the research team found "insecure, web-based interfaces to four control servers."[86] Those interfaces then allowed the exploiters to receive data from compromised computers, of which there were at least 1,295 in at least 103 countries.[87] Even more important, is the

---

80. *Id.*

81. *See generally Tracking GhostNet: Investigating a* Syber Espionage *Network*, INFORMATION WARFARE MONITOR, Mar. 29, 2009, http://www.nartv.org/mirror/ghostnet.pdf [hereinafter *GhostNet*].

82. *Id.* at 13–14.

83. *Id.* at 5.

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.*

fact that around 30 percent of those infected computers were "high-value," including:

> [T]he ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan; embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation), and the Asian Development Bank; news organizations; and an unclassified computer located at NATO headquarters."[88]

Such massive amounts of data could not easily be gathered through traditional means of espionage, and the number of people, time, and resources needed to obtain that much data through the use of spies and other traditional means would have been exorbitantly higher.

2. Much Easier and Less Expensive Access

Partly mentioned above, *GhostNet* is a great example of how easy and inexpensive it can be to conduct such extensive networks for the purposes of exploitation. As stated in the summary of the investigation into *GhostNet*, "[*GhostNet*] demonstrates the ease by which computer-based malware can be used to build a robust, low-cost intelligence capability and infect a network of potentially high-value targets."[89]

3. Unknown Effects, Spread to Unintended Targets

While the problem of unintended consequences is often discussed in relation to cyber attack, cyber exploitation can also have unintended consequences.[90] Although the exploitation may begin with a very specific target, because of the way computers become infected and then perpetuate the infection in order to gain access to more vulnerabilities and more computers, the exploitation can often end up infecting unintended targets and producing unintended results. The research team investigating *GhostNet* stated that the fact that so many high value targets were identified in *GhostNet* was likely coincidental, "spread by contact between individuals who previously communicated through e-mail."[91]

4. Attribution Is Near Impossible

Even at the end of the long investigation into *GhostNet*, the analysis never revealed who is in control of *GhostNet*, what the motivation behind

---

88. *Id.*
89. *Id.* at 6.
90. NRC REPORT, *supra* note 1, at 27.
91. *GhostNet*, *supra* note 81, at 6.

GhostNet was, how to accurately characterize the network, or even what data exactly has been exploited.[92] Because control of some of the infected computers has been traced to China, the most obvious explanation would be that the Chinese state has exploited these high profile targets for military and strategic-intelligence purposes. However, because of the uncertainty surrounding the cyber realm, acting on that assumption would be very dangerous.[93]

5. Long Time to Investigate, Few Conclusive Answers

Furthermore, because of the problems of attribution, investigations into cyber exploitation can go on for years and result in very little conclusive information. For example, with *GhostNet*, Tibetan groups first reported being targeted from servers in China back in 2002.[94] In 2005, a member of the investigation team began collecting and archiving samples of the payloads and the social engineering used.[95] Beginning in 2008, the whole investigative team began analyzing those samples.[96] Despite all this work, as stated above, the investigation team has not been able to conclusively find the actor(s) involved, determine the motivation, or find out what data has been compromised.

VII. CONCLUSION

One difference between cyber exploitation and traditional espionage that the *GhostNet* example does not illustrate is the ease with which cyber exploitations can be equipped to carry out cyber attack. This difference, combined with the reasons discussed previously, help illustrate how much more threatening cyber exploitation can be compared to traditional means of espionage. Because of this, cyber exploitation should not be treated the same as traditional espionage, and it should, even by itself, in certain instances be able to constitute a "threat or use of force." And in those instances when cyber exploitations do not rise to the level of "threat or use of force," which would likely be the majority of cases, those exploitations should largely be prohibited on the international level, not just criminalized by nations.

---

92. *Id.* at 48.
93. *Id.*
94. *Id.* at 17.
95. *Id.*
96. *Id.*