

---

---

# INTERNATIONAL LAW STUDIES

PUBLISHED SINCE 1895

U.S. NAVAL WAR COLLEGE



## Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference

*Yoram Dinstein*

89 INT'L L. STUD. 276 (2013)

Volume 89

2013

---

---

## Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference

*Yoram Dinstein\**

### I. INTRODUCTION

Truth to tell, I am more than a little bothered and bewildered by the direction taken in a considerable portion of the papers submitted to the conference and in the deliberations that ensued.

Why bewildered? The problem may be semantic, but when I was invited to participate in a conference on “cyber war,” I fully expected—as a layperson in the cyber sphere of activities—to encounter difficulties in decoding a specialized experts’ jargon with which I am not closely acquainted. Indeed, when the first speaker mentioned clouds, I thought that he was talking about inclement weather. When another participant talked about malware, it sounded to me like a reference to a breach of the dress code. What really surprised me, however, was that so many participants—while displaying the most intimate familiarity with the “cyber” vocabulary—were apparently stymied by the concept of “war.”

I should have thought that, for the military at least, the expression, “war,” is largely a no-brainer. Should it not have been self-evident to every person present that war postulates an armed conflict? Yet, panelist after panelist—even among those associated with United States Cyber Com-

---

\* Professor Emeritus, Tel Aviv University, Israel.

mand—addressed issues that pertain in a generic manner to illicit cyber operations (of heterogeneous characterizations and motivations) having no apparent linkage to an ongoing or prospective war.

This bothers me. Having been twice the victim of “phishing” expeditions into my e-mail account, I am acutely interested in what can be done to stop peacetime intrusions into somebody else’s private cyber domain. I am fascinated by the entire range of problems extending from “hacking” to grand-scale theft of intellectual property in peacetime. Nevertheless, surely, this is not why this conference was convened at the Naval War College. Our remit was “cyber war,” and this is what ought to have attracted our attention—to the exclusion of any diversionary items on anybody’s pet agenda.

As an illustration of the disorientation stoked by the departure from the straight—and—narrow meaning of “cyber war,” let me point at the rather prolonged verbal give—and—take that went on in connection with the theme of sovereignty. I freely concede that sovereignty is a topic that ought to be of interest to anyone interested in international law. I have myself written about it,<sup>1</sup> and I find the evolution of this centuries-old precept to be of compelling import. All the same, I do not propose to go into the intricacies of the matter. I would have liked to critique at length some of the peculiar notions of sovereignty advanced in this conference. I shall not succumb to the temptation for the plain reason that the subject is largely irrelevant to cyber warfare.

It must be acknowledged that the sovereignty of enemy countries in wartime is trampled underfoot without the slightest hesitation. Thus, when the United States launched its devastating “shock and awe” attack on Baghdad in 1991, did anyone in the Department of Defense spend even five seconds mulling over Iraqi sovereignty? The question is rhetorical. And, if enemy sovereignty can be totally ignored in kinetic warfare, why should it be of greater weight when cyber warfare comes into the picture? There is one salient case in which sovereignty in wartime retains its full vigor, and that is neutrality: the sovereignty of neutral States must be fully deferred to by all belligerent parties. But that is a side issue when compared to the mortal blows that the antagonists deal to each other.

What the conference ought to have concentrated on is how cyber operations bring about or are prosecuted in war. This was properly done by a

---

1. See Yoram Dinstein, *Sovereignty, the Security Council and the Use of Force*, in *REDEFINING SOVEREIGNTY: THE USE OF FORCE AFTER THE COLD WAR* 111, 111–22 (Michael Bothe, Mary Ellen O’Connell & Natalino Ronzitti eds., 2005).

number of lecturers. I shall devote my remarks to the highlights of their presentations, adding a few points of my own.

In the framework of war, cyber operations invite analysis from the respective standpoints of both the *jus ad bellum* and the *jus in bello*.

## II. THE *JUS AD BELLUM*

As far as the *jus ad bellum* is concerned, the cardinal question is not (as suggested repeatedly) whether a cyber operation rises to the level of use of force, but whether it reaches the threshold of an armed attack. The use of inter-State force is strictly forbidden in Article 2(4) of the United Nations Charter,<sup>2</sup> as well as in customary international law.<sup>3</sup> But, unless that use of force qualifies as an armed attack—pursuant to Article 51 of the United Nations Charter<sup>4</sup> and customary international law,<sup>5</sup> which lay the ground for the exercise of the right of self-defense—the response of the target State is necessarily limited in scope. As long as the use of force does not amount to an armed attack, the target State can bring the matter before the Security Council, it can employ non-forcible countermeasures or it can sue (assuming that some international court or tribunal is vested with jurisdiction). But it cannot use counterforce in self-defense.

There is a vital fork in the road facing the State that has fallen victim to an unlawful use of force. In the musical *Gypsy and Dolls*, the famous lyrics are: “Sue me, sue me / Shoot bullets through me.” Still, as anyone who is not in the musical business will readily perceive, there is a critical discrepancy between the options of “Sue me, sue me” and “Shoot bullets through me.” Consistent with Article 51, shooting bullets (as distinct from reliance on litigation), in response to the use of force, is permissible only when an armed attack occurs. I do not want to go into the thorny issue of anticipatory self-defense. Suffice it to say that I do not subscribe to the notion that anticipatory self-defense (preceding an expected armed attack) is compatible with Article 51. At the same time, I propound the legality of

---

2. Charter of the United Nations, June 26, 1945, *reprinted in* 9 INTERNATIONAL LEGISLATION: A COLLECTION OF THE TEXTS OF MULTIPARTITE INTERNATIONAL INSTRUMENTS OF GENERAL INTEREST 327, 332 (Manley O. Hudson ed., 1950).

3. *See* Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 99–100 (June 27) [hereinafter *Nicaragua*].

4. Charter of the United Nations, *supra* note 2, at 346.

5. *See Nicaragua*, *supra* note 3, at 94.

interceptive self-defense in reaction to an embryonic armed attack which has already commenced.<sup>6</sup>

A query posed by multiple interlocutors—from the dais as much as from the floor—is whether there exists a gap between Article 2(4) (use of force) and Article 51 (armed attack). My answer is definitely affirmative. I put it to you that it would defy logic to maintain that, in one of the most carefully crafted instruments in the history of international law (the Charter of the United Nations, serving as a semi-constitution of the contemporary international community), the framers resorted to divergent phraseology—“use of force,” on the one hand, and “armed attack,” on the other—to describe exactly the same phenomenon.

As we have been given to understand, the United States government apparently does not recognize the gap between Article 2(4) and Article 51. But, if so, this would be no more than a knee-jerk reaction to the fact that the gap was overemphasized in the *Nicaragua* judgment of 1986<sup>7</sup> (which the United States has many justifiable grounds to resent). I do not deny that in *Nicaragua* the International Court of Justice went too far in its assessment of the dimensions of the gap. Preeminently, the Court did not view “a mere frontier incident” as an armed attack.<sup>8</sup> I find this to be an untenable position. It was carried to its illogical conclusion by the Eritrea-Ethiopia Claims Commission’s incongruous holding of 2005, whereby border clashes between infantry units, even when leading to bloodshed, do not make the grade of an armed attack.<sup>9</sup>

In my opinion, the gap between Article 2(4) and Article 51—while there—must be seen in its right proportions. What the gap denotes is that a use of force not involving loss of life or significant destruction of property falls short of an armed attack.<sup>10</sup> If a soldier of State *A* shoots across the border of State *B*, killing a cow, this is an instance of use of force. But, absent a minimal degree of gravity, the act (albeit unlawful) does not rank as an armed attack. An armed attack must leave behind a trail of human casualties or ample destruction of property. Only when that happens is it justi-

---

6. See YORAM DINSTEIN, *WAR, AGGRESSION AND SELF-DEFENCE* 203–5 (5th ed. 2011).

7. See *Nicaragua*, *supra* note 3, at 101, 110.

8. *Id.* at 103.

9. Eritrea-Ethiopia Claims Commission, Partial Award, *Jus ad Bellum* (Ethiopia’s Claims 1–8), 2005, 45 INTERNATIONAL LEGAL MATERIALS 430, 433 (2006).

10. See DINSTEIN, *supra* note 6, at 208.

fied to have recourse to counterforce while invoking the right of self-defense (as per Article 51).

There is a certain reluctance to admit that cyber attacks—no less than kinetic attacks—may be categorized as armed attacks under Article 51. I cannot explain this attitude. Laypeople may be misguided by the invisibility of the electrons set in motion by a cyber attack. Contrarily, cyber experts may be so captivated by the act of tampering with the integrity of the target computer that they lose sight of the external lethal/destructive effects of the attack. This would be parallel to artillerymen concerned with the design of armor-piercing shells who do not ponder what havoc would happen once the projectiles have penetrated their targets.

In essence, cyber (as has been stressed in sundry presentations) must be looked upon as a new means of warfare—in other words, a weapon: no less and no more than other weapons. As with all known weapons, the test of a new weapon is not how intimidating it looks—or how ingeniously the novel mechanism works—but what harm it is liable to produce.

In its 1996 advisory opinion on the *Legality of the Threat or Use of Nuclear Weapons*, the International Court of Justice underscored that Article 51 does not refer to any specific weapon: the provision applies to (and permits self-defense in response to) all armed attacks, regardless of the weapon employed in pressing the attack.<sup>11</sup>

The same legal scrutiny should take place when the yardsticks are those of customary international law. The legal principles of the customary *jus ad bellum* remain intact whether the armed attack is kinetic or cyber. Self-defense in response to cyber armed attacks can take place under customary international law, as much as under Article 51. It is immaterial that, as yet, no explicit State practice has crystallized concerning the exercise of the right of self-defense against cyber armed attacks.<sup>12</sup> There is no need for State practice to develop separately as regards every concrete weapon employed in an armed attack.

It should be added that, when exercised against a cyber armed attack, self-defense need not be circumscribed to “cyber-on-cyber” warfare. Once a State is at war (in light of the *jus ad bellum*), it can use all the military assets available to it (within the limits of the *jus in bello*), whether they are kinetic or cyber.

---

11. *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 I.C.J. 226, 244 (July 8).

12. See Marco Roscini, *World Wide Warfare—Jus ad Bellum and the Use of Cyber Force*, 14 MAX PLANCK YEARBOOK OF UNITED NATIONS LAW 85, 123–24 (2010).

Already in 1999, at a previous Naval War College conference on computer network attacks (as they were then called), I observed that these attacks can cause fatalities through gaining control of target computers, causing a shutdown of computer-controlled life-support systems, deadly aircraft crashes, ruinous floods (by opening the sluices of high dams) and even the doomsday scenario of the meltdown of a nuclear reactor.<sup>13</sup> A lot has transpired since 1999. What looked at the end of the twentieth century to be a sci-fi fantasy is increasingly becoming a realistic script for the twenty-first century.

### III. ATTRIBUTION

No doubt, the attribution of a cyber attack to its real source may be fraught with difficulties. But is this a unique feature of cyber war? In actuality, attribution is often challenging even in circumstances of kinetic warfare, especially at sea. Reference has been made to the famous *Corfu Channel* case of 1949.<sup>14</sup> Well, what were the facts there? In 1946, two British destroyers struck mines laid in Albanian territorial waters, which are part of the Corfu Channel, an international strait between the Greek island of Corfu and the Albanian coast. The explosions caused heavy damage to the destroyers and dozens of casualties among the British sailors. Albania lost the case on the ground that it must have known of the existence of the minefield, and that it should have warned the approaching British warships of the imminent danger within its territorial waters.<sup>15</sup> Yet, interestingly, the International Court of Justice did not find sufficient evidence to establish who exactly had laid the mines (although the spoor led to the door of neighboring Yugoslavia), and pronounced that the origin of the mines remained a matter of conjecture.<sup>16</sup>

It may be added that in 1937—at the time of the Spanish Civil War—an arrangement was concluded in Nyon “against piratical acts by submarines,” perpetrated in the Mediterranean by unknown submarines and resulting in the sinking of merchant ships not belonging to the opposing parties.<sup>17</sup> This was an exceptional instrument, which treated activities by

---

13. Yoram Dinstein, *Computer Network Attacks and Self-Defense*, in *COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW* 99, 105 (Michael N. Schmitt & Brian T. O’Donnell eds., 2002) (Vol. 76, U.S. Naval War College International Law Studies).

14. *Corfu Channel* (U.K. v. Alb.), 1949 I.C.J. 6 (Apr. 9).

15. *Id.* at 22–23.

16. *Id.* at 16–17.

17. Nyon Arrangement, Sept. 14, 1937, 181 L.N.T.S. 135, 137.

submarines—i.e., government warships—as piratical, although as a rule piracy is restricted to acts committed by private persons for private ends.<sup>18</sup> The rationale underlying the Nyon Arrangement was that the submarines in question (suspected to be either German or Italian) could not be identified, and no State assumed responsibility for their depredations.<sup>19</sup>

I do not underrate the imperative need of tracing back a cyber (or a kinetic) attack to its source. It would be reckless (and senseless) to strike back hastily at the ostensible fount of a cyber attack, for the target State (State *B*) may be lashing out at an innocent party (State *C*) in lieu of the culpable actor (State *A*). However, as we were informed by the Cyber Command experts, tracing back the originator of a cyber attack is normally feasible: the catch is that it is time-consuming.

I fail to see the great peril posed by a delay in identifying the State responsible for a cyber attack. After all, if the unattributed cyber attack is an isolated event (not followed by any other attack), there is no inexorable rush to figure out instantaneously who is really behind it. Conversely, if the cyber attack is only the precursor of a stream of other attacks in its wake, source verification is likely to become much easier and faster.

Does the fact that a cyber attack is mounted without disclosure of identity instigate an ethical issue (as has been suggested)? I do not see why there is anything intrinsically wrong (at least legally) in an attacker not showing his hand overtly. In kinetic warfare, a sniper does not disclose his identity or whereabouts. Why should a cyber attacker behave differently?

Patently, the legal dissection undergoes a radical transformation if the cyber attacker does not only strike anonymously but is masquerading behind a specific false front (from which the cyber attack appears to have emanated). It then depends on the character of that fraudulent front. If it is, say, a hospital or a school, the deceitful conduct is no different from the behavior of a kinetic attacker hiding behind or among civilian “human shields.”<sup>20</sup> The *jus in bello* strictly forbids the use of “human shields” as a method of warfare.<sup>21</sup>

---

18. See the definition of piracy in Article 101 of the 1982 Law of the Sea Convention. United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 3.

19. L.F.E. Goldie, *Terrorism, Piracy and the Nyon Agreements*, in *INTERNATIONAL LAW AT A TIME OF PERPLEXITY: ESSAYS IN HONOUR OF SHABTAI ROSENNE* 225, 240–44 (Yoram Dinstein ed., 1989).

20. On “human shields,” see YORAM DINSTEIN, *THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT* 152–55 (2d ed. 2010).

21. See Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 51(7), June 8,

IV. THE *JUS IN BELLO*

Assuming that war is already raging (whether its onset was a cyber or a kinetic armed attack), the *jus in bello*—a.k.a. the law of armed conflict (LOAC) or international humanitarian law—automatically applies. We have been told over and over of the need to apply LOAC to cyber warfare “by analogy.” But, to my mind, there is no room in this context for an analogy, which by its nature is based on conceptual similarity and correspondence. There is nothing extraordinary in cyber warfare: it is just ordinary warfare with a little bit of extra. Cyber warfare does not merely resemble other forms of warfare: it is warfare. As such, it is directly governed by the *jus in bello*.

Concerns have been raised about the clarity of the LOAC *lex lata*. I find these concerns both exaggerated and unreal:

- (i) These concerns are exaggerated, because (as shown by Herbert Hart) every legal rule includes a nucleus of clarity surrounded by a penumbra of uncertainty, the meaning of which may prove doubtful in certain circumstances.<sup>22</sup> Several panelists dwelt upon the penumbra of LOAC rules. However, the nucleus of the rules is equally there.
- (ii) Scholarly doubts about the state of the *lex lata* are unreal, since they are not shared by the end users of LOAC. The armed forces of States constantly reiterate LOAC rules in their military manuals, applying and enforcing them quite rigorously. There is also a modicum of international enforcement today. The Yugoslav Tribunal (the ICTY) has already come up with extensive jurisprudence, which shows that LOAC is alive and kicking as a robust legal system.<sup>23</sup>

In keeping with LOAC, cyber operations do not automatically come within the ambit of the definition of “attacks,” which are defined as “acts of violence against the adversary, whether in offence or in defence.”<sup>24</sup> The condition of violence is *sine qua non*. Unlike an armed attack under the *jus ad*

---

1977, 1125 U.N.T.S. 3, reprinted in THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS 711, 736 (Dietrich Schindler & Jiri Toman eds., 4th ed. 2004) [hereinafter Additional Protocol I].

22. H.L.A. HART, THE CONCEPT OF LAW 11–12 (1965).

23. See, e.g., Prosecutor v. Blaškić, Case No. IT-95-14-T, Judgment (Int’l Crim. Trib. for the former Yugoslavia Mar. 3, 2000); Prosecutor v. Blaškić, Case No. IT-95-14-A, Appeal Judgment (Int’l Crim. Trib. for the former Yugoslavia July 29, 2004).

24. Additional Protocol I, *supra* note 21, art. 49(1) at 735.

*bellum*, a *jus in bello* attack would embrace my previous bovine example: if a cow is killed by enemy fire, that is an attack under LOAC. All that is necessary is death/injury to human beings or more than nominal damage to property. The same acid test is applied to all types of warfare, whether kinetic or cyber. If the consequences of a cyber operation are human death/injury or tangible property damage, it constitutes an attack compatible with LOAC requirements.<sup>25</sup>

Accordingly, a cyber operation does not pass muster as an “attack” if it is limited to (i) intelligence gathering (through collection of data and information); (ii) disruption of communications; or (iii) issuing false orders to enemy forces. I therefore fail to see why the mere planting of a “worm” in an enemy computer (without destroying it) is tantamount to an attack.

As for intelligence gathering, it must be appreciated that espionage *per se* is not prohibited by LOAC, although the individual spy (engaging in this activity behind enemy lines and out of uniform) may be punished by the enemy if he falls into its hands during such an engagement.<sup>26</sup>

Under the fundamental principle of distinction, attacks—whether cyber or kinetic—must be confined to lawful targets, to wit, combatants, civilians directly participating in hostilities or military objectives. What does this mean in concrete cyber terms?

First and foremost, direct attacks against civilian computers—or other civilian objects—are prohibited. This is the incontestable nucleus of a basic rule of LOAC governing kinetic, as well as cyber, attacks. The penumbra relates to the definition of a civilian computer. The general definition of civilian objects is negative: “all objects which are not military objectives.”<sup>27</sup> The same proposition applies also to computers: civilian computers are those that are not military computers.

Like all military objectives, military computers are defined by their “nature, location, purpose or use.”<sup>28</sup> A non-exhaustive list of military computers by nature would include (i) computers designed as components in kinetic weapons or weapon systems, e.g., in artillery, tanks, warships, military

---

25. See Michael N. Schmitt, *CNA and the Jus in Bello: An Introduction*, in PROCEEDINGS OF AN INTERNATIONAL EXPERT CONFERENCE ON COMPUTER NETWORK ATTACKS AND THE APPLICABILITY OF INTERNATIONAL HUMANITARIAN LAW 101, 112 (Karin Byström ed., 2004).

26. On espionage, see HARVARD PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rules 118–24 (2009).

27. Additional Protocol I, *supra* note 21, art. 52(1) at 737.

28. *Id.*, art. 52(2).

aircraft or missiles; (ii) computers designed to facilitate the logistical operation of military units; and (iii) computers designed for the production or supply of munitions, the development of new weapons, etc.

Run-of-the-mill computers (to wit, those that are not military computers by nature) may become military computers by use simply due to serving combatants for military purposes. This broad classification encompasses not only computers containing sensitive operational data or classified military information. Once computers are used in the discharge of military duties—even if they are dedicated to mundane administrative tasks, such as innocuous and unclassified correspondence—they are military objectives.

In case of doubt whether a computer is civilian or military, it must be viewed as civilian.<sup>29</sup> But this is not as simple as it sounds. For instance, if a civilian uses a computer that previously served a member of the armed forces, the fact that the military software has been removed does not settle the matter inasmuch as the hardware may be contaminated; the hard drive of the computer may still contain unerased military data.

Apart from direct attacks against civilian computers, LOAC interdicts indiscriminate attack. When a malicious destructive “virus” is planted in enemy military computers—absent any control over the possibility of its spreading unchecked to civilian computers—this will be considered an unlawful indiscriminate attack.<sup>30</sup> In terms of being indiscriminate, the act of planting a virtual destructive virus must be deemed to be on a par with that of planting a lethal biological virus.

Empirically, the crux of the issue in cyber as much as in kinetic attacks is proportionality in terms of collateral damage. The general rule is that when lawful targets are attacked, collateral damage to civilians/civilian objects must not be expected to be “excessive” in relation to the “concrete and direct” military advantage anticipated.<sup>31</sup> A cyber attack may in fact cause less collateral damage than a kinetic attack on the same site.<sup>32</sup> But even a cyber attack may trigger a host of civilian casualties and massive destruction to civilian objects. When will the casualties and/or destruction be considered “excessive”? Here the penumbra is more spacious than usual,

---

29. *Id.*, art. 52(3).

30. See Johann-Christoph Woltag, *Cyber Warfare*, in MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 988, 991 (Rüdiger Wolfrum ed., 2012).

31. See Additional Protocol I, *supra* note 21, art. 51(5)(b) at 736.

32. See Herbert S. Lin, *Operational Reality of Cyber Warfare*, in INTERNATIONAL HUMANITARIAN LAW AND NEW WEAPON TECHNOLOGIES 137, 140 (Wolff Heintschel von Heinegg ed., 2012).

there being no scientific way to measure when losses and damage are “excessive” compared to the military advantage anticipated. Still, it is taken for granted that the attacker must behave in a reasonable manner.

I have alluded to the need for the military advantage anticipated to be “concrete and direct,” that is to say, not just abstract or speculative. However, military advantage has to be looked at in a holistic fashion. When a large-scale attack is in progress, the outlook would be distorted if every discrete segment were assessed in isolation: it is required to put in balance the overall campaign.<sup>33</sup> Ergo, if a cyber attack is launched systematically against an entire array of enemy military computers, with dire consequences for civilians/civilian objects by way of collateral damage, the military advantage must be evaluated from a comprehensive perspective. Parsing the piecemeal benefits accruing from strikes against particular target computers may not tell the story accurately. The whole may be greater than the sum of its parts.

#### V. A NEW TREATY?

I share the view that there is no point at the present juncture in seeking to initiate a new treaty promulgating a code of conduct in cyber warfare. First, I cannot imagine that States would be ready and willing to undertake anytime soon the arduous process of formulating such a treaty. But, second, I do not think that the projected treaty (if it were to be drafted) would do more than enunciate the general norms of LOAC.

Bear in mind that this is by no means the first time in the history of LOAC that the introduction of a new weapon has created the misleading impression that great legal transmutations are afoot. Let me remind you of what happened upon the introduction of another new weapon, *viz.*, the submarine. The full potency of that weapon came to light in World War I, when the unrestricted U-boat offensive almost choked the Allied countries. In the postwar era, many voices were raised in favor of adopting a new general treaty coming to grips with this controversial innovation. What was the outcome? After two failed attempts and much soul-searching, a *procès-verbal* was successfully concluded in London in 1936. Yet, all that the authors of the *procès-verbal* managed to accomplish was proclaiming that “submarines must conform to the rules of international law to which sur-

---

33. See UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 5.4.4 (2005).

face vessels are subject” (accentuating some particulars).<sup>34</sup> I am positive that, if a treaty on cyber warfare were done today, it would similarly stipulate in an anodyne fashion that the general rules of LOAC must be conformed with.

## VI. CONCLUSIONS

Let me conclude with two interlaced observations:

- (i) We hear all the time about the asymmetry allegedly inherent in present-day LOAC, with the legal cards stacked in favor of the major powers at the expense of poor (militarily under-equipped) countries. Well, cyber warfare lends impoverished countries—ones possessing no aircraft carriers, no F-15s or 16s, and no cruise missiles—the opportunity of leveling the score. All that such a country needs is a few “whiz kids” who are capable of breaking the firewalls of the high and mighty, perhaps turning the tables on the latter. Inordinate computer dependency by the strongest nations of the world thus leads to a special vulnerability.<sup>35</sup>
- (ii) The real challenge for Cyber Command, as I see it, is to make sure that nobody will be able to turn the tables on the United States, and that the United States—the most advanced in the world, not only in aircraft carriers, F-15s and 16s and cruise missiles, but also in cyberspace—can preserve its military superiority against all actual and potential adversaries. I sincerely hope that Cyber Command is not mesmerized by entitlements to intellectual property, but instead is preparing itself—through “war gaming”—for contingencies of real war. For, if you delete “war” from the equation of “war gaming,” the only element that you are left with is “gaming.” I believe that Cyber Command should shift its gaze away from the distractions of cyber operations in peacetime. It must focus on averting a future cyber Pearl Harbor.

---

34. *Procès-Verbal* Relating to the Rules of Submarine Warfare set forth in Part IV of the Treaty of London of 22 April 1930, Nov. 6, 1936, 173 L.N.T.S. 353, 3 Bevans 298, reprinted in THE LAWS OF ARMED CONFLICTS, *supra* note 21, at 1145, 1146.

35. See Robert G. Hanseman, *The Realities and Legalities of Information Warfare*, 42 AIR FORCE LAW REVIEW 173, 191–95 (1997).