New War, Old Law: Can the Geneva Paradigm Comprehend Computers?

*Jason Beckett**

Keywords: armed conflict; arms control; international humanitarian law; strategic information warfare; use of force.

Abstract: Strategic Information Warfare (SIW) has recently begun to garner significant interest among the military and strategic defence communities. While nebulous and difficult to define, the basic object of SIW is to render an adversary's information systems inoperative or to cause them to malfunction. While information is the key, the means, and the target of SIW, real world damage is the intention and effect. It is, nonetheless, an area which has been almost completely ignored by positive international law. The purpose of the present article is to begin to resolve this *lacuna* by analysing the applicability to, and effect of, international humanitarian law (IHL) on SIW. The author makes recommendations as to possible alterations and improvements to IHL to resolve this *lacuna*.

> [In] 1956 when Khrushchev said: "We will bury the West." What he was really saying was that the military industrial complex of the Soviet Union would win out over the military industrial complex of the West – and note that it's industrial. What Khrushchev didn't understand was that 1956 was the first year in the United States that white-collar and service employees outnumbered blue-collar workers. [...] The industrial complex, military or not, was at its end point.
>
> *Alvin Toffler, Novelist and Social Theorist*[1]

1. INTRODUCTION: RELIANCE ON INFORMATION TECHNOLOGY, AND THE INTERDEPENDENCE OF COMPUTER BASED INFRASTRUCTURE

To facilitate consideration of SIW, an overview of information dependence, and critical infrastructure interdependencies, along with a brief description of the Internet shall be presented to set the scene. Then the lessons of past wars, and

* Research assistant at the University of Glasgow, where this article was originally written in partial fulfilment of an LL.M. degree. Thanks go to Dr I.G.M. Scobbie for support, help, and advice, and to Mr D. Goldberg for introducing me to the concept of SIW. Needless to say, any remaining errors are my own.

1. Speaking in BBC Discussion program, *The I-Bomb* – Horizon BBC2 – 27 March 1995. Transcript available at http://helios.njit.edu:1994/cgi-bin/contrib/interdependence/ibomb.htm.

13 Leiden Journal of International Law 33-51 (2000)

the complimentary evolutions of war and IHL shall be considered, before the modalities of SIW and the applicability of IHL to them are analysed.

Modern society is living through the information revolution, whose exponential advances have already created an Information Age. This has resulted in a growing dependence on computers to store, refine, and distribute this information; the 'oil', or key resource, of the modern world.

> The development of the computer and its astonishingly rapid improvements have ushered in the Information Age [...] Our security, economy, way of life, and perhaps even survival, are now dependent on the interrelated trio of electrical energy, communications, and computers.[2]

Although the development of computers, and the advances of the information age, have proved beneficial, they are not an unalloyed good. Computers, and the internet, have opened up a wealth of new opportunities, but with these have come new dangers.

> National security is becoming progressively more dependent on and identified with assets related to the 'information revolution.' As part of this revolution, both defense and civilian activities are becoming more heavily dependent on computers and communications, and a variety of key information systems are becoming more densely and extensively interlinked. [This creates] the capability for strategic information warfare.[3]

2. EXISTENCE AND IMMANENT GLOBALITY OF THE INTERNET

These problems, or dangers, are greatly exacerbated by the existence of the Internet, a global communications network which is not intrinsically restricted to peaceful use. Globality, and 'a-jurisdictionality' are the defining characteristics of the internet, of whose evolution and current form Professor Post offers the following description:

> The Internet was designed to withstand nuclear attack. The RAND Corporation designed the network to be a decentralized command-and-control-and-communications system, one that would be less vulnerable to missiles than a system commanded by a centralized headquarters [...] [it] was designed without a centralized control mechanism or any single location through which all internetwork traffic must travel, all network nodes are [...] equally capable of performing the key internetwork message routing functions. [Thus] the Internet is not merely multi-jurisdictional it is almost 'a-

2. President's Commission on Critical Infrastructure Protection (PCCIP Paper), Report available at http://www.pccip.gov/report_index.html.
3. RAND Corporation Report, Cyberwar is Coming, Report available at http://www.rand.org/ publications/RRR/RRR.fall95.cyber.

> jurisdictional' physical location, and physical boundaries, are irrelevant in this networked environment.[4]

It is this globality, and the uncontrolled nature of internet traffic, which makes SIW such a danger, as an attack can be launched from anywhere, against a target anywhere, at any time; physical location and military strength become irrelevant. As a senior US government commission has noted:

> [while it] is not surprising that infrastructures have always been attractive targets for those who would do us harm. In the past we have been protected from hostile attacks on the infrastructures by broad oceans and friendly neighbors. Today, the evolution of cyber threats has changed the situation dramatically. In cyberspace, national borders are no longer relevant. Electrons don't stop to show passports.[5]

3. EVOLUTION OF WARFARE AND THE LESSONS OF PAST WARS

War has been going on at some level for as long as mankind has existed in organised societies which have been forced to protect their resources from others. Historians have tended to divide the evolution of warfare into three distinct periods, or waves.[6] First wave warfare was agrarian, pre-industrial, feudal war. Then came the industrial revolution, mass production changed the face of the earth, and warfare was inevitably affected. This was second wave, or industrial, warfare. Its objects became grander, and its destructive capacities grew exponentially.

However, what previous wars, and particularly the Second Gulf War – in which a large and reasonably well equipped army was destroyed with a minimum of loss and a true minimum of effort – have shown is, ultimately, that the superpowers, or at least the USA, cannot be defeated in a conventional manner. Coupled with assured extinction under the MAD[7] doctrine of thermo-nuclear warfare this should demonstrate to would be 'new powers' that new methods of warfare must be sought.

> The Gulf War provided a clear lesson learned for all would–be regional hegemons: Don't take on the U.S. and its allies on a traditional conventional battlefield. There are other approaches, other means and strategies [...] so-called asymmetric strategies

4 D. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, J. Online L. (1995), Art. 3, paras. 35-36 [paragraph breaks suppressed].

5. *See* PCCIP Paper, *supra* note 2.

6. *See* R. Haeni, An Introduction to Information Warfare, available at http://www.seas.gwu.edu/student/reto/infowar/info-war.html .

7. Mutually Assured Destruction; this refers to the idea that a nuclear war cannot be survived, let alone won, but must inevitably escalate until the destruction of mankind, and quite probably the planet, ensues.

https://doi.org/10.1017/S0922156500000030 Published online by Cambridge University Press

> such as those involving the use of biological or chemical weapons [...] SIW offers a new element.[8]

This, SIW, is third wave warfare, the entry costs are relatively modest and it is inherently most likely to be effective against the technologically advanced states, i.e. those, like the USA, who are otherwise essentially invulnerable. SIW also falls outwith the classic defence paradigm, as "reliance on any [conventional] kind of deterrence strategy [...] assumes an ability to unambiguously identify an attacker"[9], which may prove impossible owing to the nature of Net based SIW attacks. Further, while the other so-called asymmetric strategies are regulated, or prohibited, by positive international law, SIW remains potentially untouched, as its weapons and destructive capacities may go unrecognised within the 'use of force' paradigm.

4. HISTORY, EVOLUTION, AND PROSPECTS OF SIW

Information has always been a prominent feature of warfare. From the earliest of times wars were portrayed as epic conflicts between 'good' (i.e. 'our side') and 'evil' (i.e. 'the other side') rather than as resource conflicts. This has continued and evolved through the use of propaganda, espionage and misinformation, each of which is regulated by current IHL.[10] Throughout this evolutionary process, intelligence agencies were formed and developed, information became a vital part of conflict and the quest for victory, as did its communication: "[c]ommunications without intelligence is noise; intelligence without communications is irrelevant."[11]

However, communication has, to date, always been seen as a means of enhancing the efficiency, or effectiveness, of traditional – guns and bombs type – warfare. A representative overview of current military perceptions of SIW and its place in war can be garnered from the following collage of the opinions of three senior US army officers:

> Upgrading our existing weapon systems to make sure that we get this information technology embedded in all of our weapon systems [...] So we have this horizontal technology integration to get this common view of the battlefield [...] [but, there is]

8. R. Molander & S. Siang, The Legitimization of Strategic Information Warfare: Ethical Considerations, available at http://www.rand.org/publications/MR/MR661/MR661.html .
9. *Id.*
10. Spies are regulated under Hague Convention IV of 1907, annexed Regulations (Arts. 29-31), Geneva Convention IV (Arts. 5 and 68), and API (Arts. 45-6) which also consider Ruses of War; all *reprinted in* A. Roberts & R. Guelff, Documents on the Laws of War (1989). Propaganda is regulated by the Convention on the International Right of Correction, adopted by UNGA resolution 630 (VII) 1952, UN Doc. A/RES/630 (VII).
11. General A.M. Grey, USMC. Quoted in the Institute for the Advanced Study of SIW, Transcript available at http://www.psycom.net/iwar.1.html.

https://doi.org/10.1017/S0922156500000030 Published online by Cambridge University Press

> absolutely no way that information-age technology can replace the soldier [...] [because] War is a dirty, personal thing, and the soldier is at the centre of that. [Therefore] War will [continue to] mean putting your soldiers on the ground and fighting each other – [albeit] with weapons which may be leveraged and more effective because of information-age technology.[12]

This is an evolution of second wave warfare, from technology in war to technological warfare, rather than true SIW. As M. Libicki, a Senior Fellow at the National Defense University, observed:

> Digitising the battlefield might be necessary for the way that we might want to fight future wars, but if we're still thinking of fighting wars around very visible platforms, such as tanks, in fact we may be putting our money in the wrong direction. Perhaps we should be thinking about not neccssarily how we make the tanks smarter, but how we use [SIW] to conduct operations without having to use the tank at all.[13]

Although virtually unnoticed, the potential for this radical evolution has long existed, the technology has simply been 'misdirected' into improving, rather than replacing conventional (and nuclear) weaponry.

> Looking back before looking forward on this matter, the path followed from the development of the ARPANET[14] through the emergence of the hacking community and culture, in parallel with ever evolving tools and techniques of electronic warfare for military ends, seems understandable enough. But the consequences of this path, and the larger implications for society and the future of warfare are only now beginning to reach national and international consciousness.[15]

This, however, is down to oversight, rather than any imaginary nature of the problem. Indeed the RAND Corporation, after running simulation exercises commissioned by the US government and Military establishment, noted that "the tendency of the exercise participants was to view information infrastructure vulnerabilities and the potential for strategic information warfare far more seriously the more they learned about the subject and debated its implications."[16]

Their solutions and suggestions for the problem were not radical, or even terribly new, but perhaps an ominous significance can be read into the implicitly analogous type of attack that inspired them.

> One promising means for instituting [...] preparedness could involve the concept of a 'minimum essential information infrastructure' (MEII). The MEII is conceived as that minimum mixture of U.S. information systems, procedures, laws, and tax incentives

12. Colonel Warden, Generals Sullivan and Salamon, on *The I-Bomb*, *supra* note 1.
13. *Id.*
14. The ARPANET is the original network designed by RAND which gradually developed into the modern day Internet.
15. Molander & Siang, *supra* note 8.
16. RAND Corporation, *supra* note 3.

https://doi.org/10.1017/S0922156500000030 Published online by Cambridge University Press

> necessary to ensure the nation's continued functioning even in the face of a sophisticated [SIW] attack [...] to reduce their infrastructure's vulnerability and/or to ensure rapid reconstitution in the face of [SIW]-type attacks. The analogue for this concept is the strategic nuclear Minimum Essential Emergency Communications Network (MEECN).[17]

As well as illustrating the extent of the modern dependency on computer related infrastructures and their vulnerability and interdependence, RAND's approach highlights and reflects the current concentration on the security aspects of SIW and demonstrates precious little concern for the legal niceties involved. Nonetheless, computerised infrastructures exist, and are growing in importance, possibly also in interdependency and vulnerability; they do, in short, make very tempting potential targets.

5. MODALITIES OF SIW

Wars can, perhaps even ought to be 'fought' without a resort to force in the traditional 'guns and bombs' sense. This does not, however, necessarily mean, or even imply, that they can be conducted without loss and suffering, it simply envisages new methods with which to bring about the defeat or subjugation of enemies – the ultimate ends of warfare.

SIW does not entail the removal of weapons, but rather their replacement, which would be facilitated by the creation of new, computer based, weapons used to attack new, computer based, targets; like a simulation or video game, but with very definite, very intentional, real world results.

> Information warfare is the offensive and defensive use of information and information systems to exploit, corrupt, or destroy, an adversary's information and information systems, while protecting one's own.[18]

In other words, SIW is the use of computers and software (viruses, worms, etc) to hack into and damage or change the control systems of key components of the adversary's electronic infrastructures, in order to weaken their position; be it military or economic, or capacity to govern their State. An integral feature of true third-wave warfare may be that there is no need to destroy anything at all, because the targets will not even be computers themselves, but rather the world to which they give access. Thus, through the proliferation of technology, wars will be fought in the battlefields of cyberspace, the place which connects all of the computers world-wide:

17. *Id.*
18. Institute for Advanced Study of SIW, *supra* note 11.

> As we move towards the third wave, and societies become more internally complex, more and more information is needed to handle routine events. Information is the central resource [...] With over a hundred million computers tying our communications, finance, transportation and power system together, we face a potential electronic Pearl Harbour [...] A threat that challenges all the traditional notions of warfare [...] In an electronically interdependent world a virtual act of war may be taken as seriously as a bomb might have been 50 years ago. If we use electronic technology to zero Gaddafi's bank account, is that an act of war?[19]

Such 'combat' would be SIW, true, third wave warfare. However, SIW need not be limited to such 'bloodless' targets; electrical power could be shut down, with (collateral or intentional) side-effects such as blinding air traffic control (which could even be attacked directly) or depriving a hospital of essential electrical power. SIW is ultimately a mode of warfare, and no war is complete without suffering. Indeed, SIW may even see the level of suffering increased, as it is fought in "four distinct separate theaters of operation: the battlefield per se; allied 'Zones of Interior' [...]; the intercontinental zone of communication and deployment; and the [...] Zone of Interior."[20]

6. THE IHL PARADIGM AND ARMED FORCE

Ever since Henri Dunant witnessed the suffering and slaughter of the battle of Solforino, and determined to create (what was to become) the International Committee of the Red Cross, IHL has been a reactive subject, in the sense that its evolution has been spurred primarily by those shortcoming in the existing regulations that each new conflict has highlighted.

> The history of development of this branch of international law is largely one of reaction to bad experience. After each major war, the survivors negotiate rules for the next war that they would, in retrospect, like to have seen in force during the last war.[21]

Thus first wave warfare was essentially unregulated, with a few exceptions for chivalry and the recognised privileges of rank and birth, as well as some "rules restricting the right of belligerents to inflict injury on their adversaries."[22]

---

19. A. Toffler, Narrator, J. Morris, and W. Schwartau, on *The I-Bomb*, *supra* note 1 [paragraph breaks suppressed].
20. RAND Corporation, *supra* note 3.
21. G. Aldrich, *Some Reflections on the Origins of the 1977 Geneva Protocols*, *in* C. Swinarski (Ed.), Studies and Essays on International Humanitarian Law and Red Cross Principles in Honour of Jean Pictet 129 (1984).
22. D. Schindler, *The International Committee of the Red Cross and Human Rights*, International Review of the Red Cross 3, at 4 (1970). For a brief overview of 'IHL' in first wave warfare, *see* H. McCoubrey & N. White, International Law and Armed Conflict 193-194 (1992).

> It was only in the nineteenth century, when wars were waged by large national armies, employing new and more destructive weapons and leaving a terrifying number of wounded lying helpless on the battlefield, that a law of war based on multilateral conventions was developed.[23]

During this time the evolving IHL appeared to be playing a constant game of 'catch-up' with the atrocious realities of evolving warfare. Regulation of second wave warfare evolved a step behind the warfare itself, e.g. the four Geneva Conventions of 1949, which sought to alleviate the deficiencies demonstrated by the unprecedented destruction and depravity of World War II. Likewise, clear echoes of the de-colonisation process and the Vietnam experience are discernible in Additional Protocol I of 1977 (API).[24]

However, in tension with this reactive nature stands the acknowledged incompleteness and 'non-atomised nature' of IHL. This and its corollary the Martens Clause[25] (and its progeny[26]) can be seen to add an element of ongoing dynamism to the regulation of conflict, and to the humane protection of civilians and combatants alike. Also in this stream stand the prohibitions of weapons as yet undeveloped or unused in battle,[27] and the proactive nature of Article 36 API.[28]

It is clear that as long as SIW only involves making existing types of weapons smarter their use will be a resort to force, and the applicability of IHL will not be in doubt. After all, this will remain second wave warfare, for and from which IHL has evolved. However, this changes fundamentally when SIW begins to replace rather than improve existing weaponry, i.e. with the evolution of 'true' SIW; "'war' without using a tank at all, not only by using the technology

---

23. *Id.*
24. *Id.*, at 131.
25. This clause, appearing in the Preamble to the Hague Convention IV of 1907, reads: "Until a more complete code of the laws of war has been issued, the high contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilised peoples, from the laws of humanity, and the dictates of the public conscience." This clause is generally perceived as bringing an ongoing, dynamic, element into IHL. *See* H. Strebel, *The Martens Clause, in* R. Bernhardt (Ed.), Encyclopaedia of Public International Law, Vol. III, at 326-327 (1997).
26. I.e., the provisions in subsequent IHL treaties clearly derived from the Martens Clause; e.g. the 1925 Geneva Gas Protocol preamble, paras. 1 and 3; the 1949 Geneva Conventions, 1 Art. 63(4), 2 Art. 62(4), 3 Art. 142(4), 4 Art. 158(4); API Arts. 1(2) and 36; the 1980 Conventional Weapons Convention preamble para. 5. All *reprinted in* Roberts & Guelff, *supra* note 10.
27 *See* St Petersburg Declaration, *reprinted in* Roberts & Guelff, *supra* note 10,, at 29; and Protocol IV to the 1980 UN Convention on Conventional Weapons on the prohibition of blinding laser weapons, United Nations CCW/Conf.1/7.
28. Article 36 reads: "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."

to make the tank smarter."[29] True third-wave conflict may necessitate a reassessment of the triggers for the application of IHL.

Until 1949 the laws of war (as IHL was then known) were applicable only in those uses of force comprising 'war in the legal sense'.[30] Among the great advances heralded by the Geneva Conventions of 1949 was the extension of applicability to "armed conflicts"[31], "even if the state of war is not recognised".[32] API explicitly adopts the same trigger, and also creates peacetime obligations of preparation.[33]

The applicability of IHL to SIW thus depends on whether SIW is construed to fall within the use of force paradigm, or should rather be seen as a 'peaceful' measure of coercion, not amounting to a use of force.[34] In terms of the *ius ad bellum* this would manifest itself in a perception of the initiation of SIW as either a breach of Article 2(4) UNC, or a 'mere' prohibited intervention.[35] For the applicability of the *ius in bello* the pertinent question becomes whether or not an Information War is an 'armed conflict'. The two questions are essentially synonymous, any use of force is regulated by IHL.[36]

The commentary to common Article 2 of the 1949 Geneva Conventions – the war or armed conflict trigger, determining the conventions' applicability – offers little help, informing us only that the conventions are applicable "from the actual opening of hostilities" and that these are constituted by "any difference [...]

29. Haeni, *supra* note 6, at para. 5.1.
30. *See* F. Kalshoven, Constraints on the Waging of War 27 (1987).
31. This conflation of 'use of force' and 'armed conflict' is assumed in the present paper, as otherwise a first use of force need not be regulated by IHL; e.g. State A launches a nuclear strike on State B, completely annihilating B. This is clearly a use of force, but where is the 'armed *conflict*'? This apparent inconsistency can be explained by reference to the differing paradigms in which the Charter IHL were drafted and justifies an expanded interpretation of 'armed conflict' to cover all uses of force. A similar result could be reached by manipulation of the duty, in common Art. 1, to "respect the [Geneva] Convention[s] in all circumstances." However, the terminological confusions and conflations between IHL and the *ius ad/contra bellum*, although deserving fuller consideration, are outside the scope of the present article.
32. Common Art. 2, Geneva Conventions of 1949.
33. *See* Art. 58, more fully considered *infra* paragraph 7.
34. It should be noted that peaceful and forceful measures are defined and distinguished by their means, rather than their results. Therefore the legal nature of SIW cannot necessarily be ascertained from its destructive capacities or potential.
35. Thus, the Friendly Relations Declaration, UNGA Res. 2625 (1970), UN Doc. A/RES/2625 (XXV), *reproduced in* I. Brownlie, Basic Documents in International Law 36 (1995), differentiates between (armed) force and "economic, political or any other type of measures used to coerce another state". *See further* A. Randelzhofer, *Article 2(4)*, *in* B. Simma (Ed.), The Charter of the United Nations: A Commentary 112 (1993).
36. This is implicit in the recent Legality of The Threat of Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, 1996 ICJ Rep. 3; *see*, e.g., para. 42: "a use of force that is proportionate under the law of self-defence, must, in order to be lawful, also meet the requirements of the law applicable in armed conflict which comprise in particular the principles and rules of humanitarian law", and para. 47: "If the envisaged use of force is itself unlawful, the stated readiness to use it would be a threat prohibited under Article 2, paragraph 4".

leading to the intervention of armed forces". However, subsequent practice, *inter alia*, the use of cruise missiles, illustrates that an actual cross-border movement of *troops* is not necessary. This highlights two points: the cross border use of weapons constitutes an armed conflict in terms of the Geneva Conventions; and, more generally, the laws of war retain a dynamism in their application. Thus, although SIW is undoubtedly a conflict it is unclear whether it can be construed as an *armed* conflict.

This question has, quite simply, *not been addressed*; either by writers or international tribunals.[37] The focus has remained on which traditional uses of force amount to armed conflict, and on the differences between internal[38] and international armed conflict. Thus in the ICTY:

> According to the Appeals Chamber Decision [...] an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State.[39]

However, the Appeals Chamber also noted that:

> This body of law is not grounded on formalistic postulates [...] Rather, it is a realistic body of law, grounded on the notion of effectiveness and inspired by the aim of deterring deviation from its standards to the maximum extent possible.[40]

This leaves open the possibility that the treaties could be interpreted so as to apply to (and hence constrain and regulate) SIW. In general, treaties are interpreted textually,[41] the words are neither added to nor subtracted from, they are simply given their 'natural meanings'; but from where should these be drawn?

The absence of a legal source bearing on this issue necessitated resort to the Oxford English Dictionary, which defines "armed" as "equipped with weapons", which are in turn defined as "instrument[s] used or intended to inflict bodily harm". It is interesting that weapons are defined by use rather than immanent characteristics, or features of design. Nonetheless, such a definition finds clear

37. However, the closely related question of what amounts to a "use of force" in terms of Art. 2(4) UNC has been very restrictively answered by Randelzhofer, *supra* note 35, at 113-114, who very clearly takes the view that it is the means and not the end which determine a breach of Art. 2(4). The applicability of this reasoning to IHL is, however, at best doubtful, given the entirely different scope and aims of the two branches of law.
38. Internal Armed Conflict, or "armed conflict not of an international character" is considerably less regulated than international armed conflict, however there are rudimentary constraints and standards encapsulated in common Art. 3 to the Geneva Conventions, and these are expanded, although also in some ways limited, in the APII of 1977.
39. *See* Prosecutor *v.* Tadić, Trial Chamber Judgement, Case No. IT-94-1, 7 May 1997, para. 561.
40. *See* Prosecutor *v.* Tadić, Appeal Chamber Judgement, Case No. IT-94-1, 15 July 1999, para. 96.
41. *See* Employment of Women in the Night Case, (Advisory Opinion), Judgment of 15 November, 1932 PCIJ (Ser. A/B) No. 50.

support in the UK legislation regarding the possession and use of weapons,[42] where the use of improvised weapons (e.g. baseball bats) is seen as every bit as unlawful as that of purpose built weapons; this conception of weapons also has some direct support in international law.[43]

An alternative method of treaty interpretation is the teleological approach.[44] This involves discerning the 'object' of the treaty, and interpreting its provisions so as to further this objective. This is essentially analogous to the so-called mischief rule of statutory interpretation.[45]

It is thus perfectly possible, using either a textual or a teleological approach to interpretation, to construe SIW as an armed conflict. The dynamism afforded by the Martens clause would allow such an evolving definition of the concept of a weapon to be included in IHL. This can be buttressed by reference to Article 38 (1)(c) of the statute of the ICJ, showing a general principle of law defining weapons by use or effect rather than by design or intrinsic characteristics. Finally, McCoubrey and White suggest looking, in cases of doubt, to the intent, or *animus belligerendi*, of the parties to the conflict, and suggest that the key to "armed conflict" is the taking of "active and hostile military measures" with 'military' being defined purely to denote state sponsored.[46]

While persuasive, there is no reason to consider these arguments compelling. The *ius in bello* is triggered by the existence of an 'armed conflict', which is implicitly equated with the *ius ad bellum* being superseded, and this occurs only where there has been a "use of force". As the interplay between Articles 41 and 42 UNC aptly demonstrates a use of force is defined by modality, not by result. Thus an overflight of enemy territory by an airforce squadron, involving no combat, strafing, bombing etc. would be a use of force – dearth of damage notwithstanding – whereas the creation of conditions of starvation and disease through the over-zealous use of sanctions under Article 41 UNC would not.[47] Furthermore, so-called economic warfare is not considered as a use of force contrary to Article 2(4) UNC, its destructive and harmful capabilities notwithstanding.[48] Oppenheim/Lauterpacht could be seen to take this point further, as

42. *See* Prevention of Crime Act 1953, s. 2.
43. *See* Meyorwitz, *infra* note 55, and accompanying text.
44. *See* Prosecutor *v.* Furundžija, Case No. IT-95-17/1, Trial Chamber, 10 December 1998, paras. 253-254.
45. *See* Prosecutor *v.* Čelebići, Case No. IT-96-21, Trial Chamber II, 16 November 1998, paras 158-165, esp. paras. 163-164.
46. *See* McCoubrey & White, *supra* note 22, at 194-195.
47. This latter could however be construed as genocide, as "deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part", but this proves little, as genocide, as "a crime in time of peace as well as war" is not strictly a part of IHL. It is nonetheless apparent that genocidal conduct carried out by SIW would be clearly criminal.
48. Randelzhofer contends that Art. 2(4) is a limited prohibition exclusively concerned with "military force", *supra* note 35 and accompanying text.

their analysis of the "economic weapon" in warfare implicitly exempts such 'force', as non-armed, from the duties of distinction and discrimination.[49]

Given the generally reactive nature of IHL – viewing the Martens Clause as primarily a reminder of the non-atomised nature of international law, and of the continued applicability of other aspects of, particularly customary, international law to the protection of those affected by war – it seems unlikely that those advocating or using such a totally new means of engagement would consider it as regulated, let alone proscribed, by existing positive international law.

Although the St Petersburg Declaration of 1868[50] declared "the only legitimate objective of war is to weaken the military forces of the enemy", it did not declare this objective to be the exclusive prerogative of war. Furthermore, common Article 2 of the Geneva Conventions also contains a provision applying their provisions to unresisted occupations. From this it could be argued *a contrario* that the use of actual, physical, military force is a *sine qua non* for the application of the conventions in the absence of territorial occupation.

There is also something incongruous about deeming a soldierless and gunless engagement an 'armed conflict'. The designation 'war' in SIW does not alter this, and is unlikely to be a legal standard, amounting to "war in the legal sense". Even if it were, a declaration of war is now felt to be neither a necessary, nor even a sufficient, circumstance for the existence of an armed conflict.[51]

Finally, however, it is worth considering the possibility that SIW may be used by a party to a conventional second wave war as an additional element to its offensive or defensive capacities. It is not difficult to envisage Saddam Hussein or Slobodan Milošević, (responding to what they would perceive as western aggression) realising that they cannot hope to defeat the US or NATO conventionally, resorting to SIW attacks on the US mainland, should such capacities become available to them. In this case IHL would already have been 'triggered', and would be applicable by virtue of the ongoing second wave war. Thus the question would re-focus to IHL's direct application to the tools of SIW, and whether they amounted to, and could be regulated as, means and methods of warfare.

7. ASSUMING APPLICABILITY: IHL'S CAPACITY TO REGULATE SIW

All unilateral actions must be proportionate to retain legitimacy,[52] however, only uses of force – i.e. those actions regulated by IHL – need *also* to meet the duties

49. *See* H. Lauterpacht, Disputes War and Neutrality, Oppenheim's International Law, Vol. II, at 208 (1952).
50. *See supra* note 27.
51. *See* McCoubrey & White, *supra* note 22, at 154.
52. It would appear that 'peaceful' Security Council mandated action under Arts. 39 and 41 UNC does not share this requirement of proportionality.

https://doi.org/10.1017/S0922156500000030 Published online by Cambridge University Press

of discrimination in effect, and the regulation of means and methods encapsulated in IHL. Thus, placing SIW within the IHL paradigm has clear benefits for mankind and civilisation. This is not impossible to presume, as, even if "not watertight", the aim of the trigger provisions of the 1949 Geneva Conventions was to do away "once and for all with the possibility for States to place such a narrowly legalistic construction on the single word 'war', and to have replaced it with a factual, objectively ascertainable notion",[53] i.e. whether there is or is not an 'armed conflict' going on. Thus the intent was manifestly to extend the protections of IHL and to limit the suffering caused by international conflict. SIW is clearly a conflict with the potential to cause much suffering and death, and so ought to be covered.

This argument can be reinforced by considering a resort to SIW within an ongoing conventional conflict. In such circumstances IHL is already applicable by virtue of the pre-existing uses of force. As a result (assuming the belligerents to be parties, or the relevant aspects of the treaty to have spawned identical custom[54]) Article 51 of the first 1977 Protocol, Additional to the Geneva Conventions of 1949 (API) proscribes certain means and methods of warfare. The official commentary explicitly equates the meaning of this phrase with that used in Article 35. Several points emerge from this: the prohibitions are not limited to "weapons in the technical sense", but may rather be understood as referring to "any device, whatever it may be"[55]; also, methods can be proscribed regardless of the legality of the tools with which they are implemented. It is thus clear that SIW attacks targeted on civilians or civilian objects, or launched indiscriminately, would be prohibited. It would be illogical to regulate the use of SIW through IHL if the former is not a species of armed conflict. It is also downright paradoxical to assume that resort to SIW in time of war should be constrained while a similar resort in time of peace should not.[56] Therefore, "the task that is surely at the heart of the question [is] the systematic application of the relevant law to [the problem at hand]. What [should be] done is to explain, elaborate and apply the key elements of humanitarian law [to SIW]."[57]

---

53. F. Kalshoven, *supra* note 30, at 27.
54. Oeter claims that Arts. 51-60 of API are generally perceived as binding customary law, *see* S. Oeter, *Methods and Means of Combat*, *in* D. Fleck (Ed.), The Handbook of Humanitarian Law in Armed Conflicts, at 109 (1995). On the possibility of simultaneous, identical, treaty and customary law generally, *see* M. Villiger, Customary International Law and Treaties (1997), chapters 5 and 6; *cf. also* Military and Paramilitary Force in and Against Nicaragua, (Nicaragua *v.* United States of America), Judgment of 27 June 1986, 1986 ICJ Rep. 14, paras. 182-189.
55. H. Meyorwitz, *The Principle of Unnecessary Suffering and Superfluous Injury*, Review of the Red Cross 98, at 103 (1994).
56. On a similar note, *see* Roberts & Guelff, *The U.S. Understanding of the Use of Teargas Under the Geneva Gas Protocol 1925*, *supra* note 10, at 137-138. On the related dangers of not treating SIW as a use of force capable of amounting to an armed attack, *see infra* note 74 and accompanying text.
57. R. Higgins, Dissenting Opinion, Legality of the Threat of the Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, 1996 ICJ Rep. 3, at paras. 9-10 [break suppressed].

Thus a basic premise of modern IHL, the duty of discrimination, should, along with the corollary prohibitions on attacks on the civilian population, civilian objects, and objects necessary to the survival of the civilian population, be applicable to SIW. Such application may not, however, prove an easy task.

> Envision a nation developing – and implementing through brandishing or actual use – a capability to disrupt the delivery of services from critical infrastructures. Try further, in a fast moving information technology (IT)-driven environment, to envision that those who would offer such tools and techniques of strategic warfare [...] to decision-makers would be able to forecast accurately the collateral effects and overall consequences of an attack of any strategic magnitude. The first is readily conceivable; the second is almost inconceivable [...] It is not hard to construct very sobering scenarios in the light of these considerations. A supposedly limited precision attack on a segment of an electric power grid could have the unintended consequences of widespread power outages and the failure of emergency power services at places like hospitals and other critical facilities.[58]

This lack of infrastructural distinction between the military and the civilian – the legitimate and the prohibited objects of attack – was also noted by the President's Commission on Critical Infrastructure Protection.[59] An interesting question which arises is, given the doctrines of proportionality and foreseeability, and the poorly understood infrastructural interdependencies, who is liable for an unforeseen chain reaction; the attacker for failing to discriminate, or the attacked for failing to distinguish?

Article 58(b) places on the parties to API a clear obligation, applicable in time of peace as well as war, not to endanger their civilians by locating military objectives "within or near densely populated areas". Given the a-spatial nature of networked computer infrastructures, this would be more aptly interpreted as an obligation to separate military and civilian infrastructures, and particularly to isolate those infrastructures indispensable to the survival of the civilian population. This could also be seen as a "necessary precaution [...] to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations."[60] Furthermore, Article 51(7) prohibits the use of civilians to shield military objectives.

The situation may not be so clear cut as regards a putative attacker, although Article 51(8) makes manifest that a breach of these duties does not legitimise an attack on civilians or civilian objects, nor does it release the adverse party from any duties toward civilians. However, the issue under consideration is not an attack on the civilian population, or civilian objects, *per se* but the related duty of distinction and the corollary notion of collateral damage.

---

58. Molander & Siang, *supra* note 8. It is notable that even where discussion of SIW moves outwith the defence/strategy paradigm, law and legal niceties are conspicuous only by their absence.
59. *See* PCCIP Paper, *supra* note 2.
60. Art. 58(c), Additional Protocol I to the 1949 Geneva Conventions.

> Thus, given continued poor understanding of infrastructure interdependencies, can SIW attacks under such 'imprecisions' be justifiable? [...] In such circumstances, what is 'acceptable' and 'fair' within the ethics of war as currently judged by civilization?[61]

Although it rarely occurs to military strategists that war itself may be regarded as abhorrent and unethical by civilisation, the question at hand is not one of fairness, but of legality. Only Article 58 provides clear obligations, and these fall on the party to be attacked.

The concept of collateral damage is best viewed as a microcosm of the uneasy balance between the necessities of war and the laws and dictates of humanity. Under this concept, Article 51(5)(b) provides that an attack on a military objective can only be considered indiscriminate, and hence illegal, if it "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

Although drafted in a manifestly subjective manner, this provision must be read in context. Article 57 places the attacker under positive duties to take "constant care [...] to spare the civilian population, civilians, and civilian objects", to "do everything feasible to verify that the objectives to be attacked" are legitimate, and to "take all feasible precautions [...] with a view to avoiding, and in any event minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects."[62] It is therefore clear that the *prima facie* indeterminate and subjective approach of Article 51(5)(b) is in fact subject to a further implicit duty to act reasonably on the best available information. However,

> [t]he energy and communications infrastructures especially are growing in complexity and operating closer to their designed capacity. This creates an increased possibility of cascading effects that begin with a rather minor and routine disturbance and end only after a large regional outage. Because of their technical complexity, some of these dependencies may be unrecognized until a major failure occurs.[63]

While this does little to determine whether a specific use of SIW will be legal, it does bring the related question of the 'intrinsic legality' of SIW to the fore. It is unclear to what extent this will be predetermined by SIW's potential inability to determine or limit, let alone define, the effects of an attack in advance;[64] i.e. its *prima facie* inherently indiscriminate nature.

> The requirement that a weapon be capable of differentiating between military and civilian targets is not a general principle of humanitarian law [...] but flows from the basic rule that civilians may not be the target of attack. [...] For this concept to have a

61. *Id.*
62. Art. 57, Additional Protocol I to the 1949 Geneva Conventions.
63. *See* PCCIP Paper, *supra* note 2.
64. I.e., the inability to predict contingent infrastructural effects, when the inter-relations of complex communications/information/power/computer infrastructures are unclear.

> separate existence, distinct from that of collateral harm (with which it overlaps to an extent) [...] it may be concluded that a weapon will be unlawful *per se* if it is incapable of being targeted at a military objective only, even if collateral harm occurs [...] To the extent that a specific [...] weapon would be incapable of this distinction, its use would be unlawful.[65]

While it is clear that there is little inherent indiscriminacy in computers or code (the 'weapons' of SIW), the requirement of distinction applies equally to methods of warfare. A clear potential for inherent indiscriminacy is created by the failure of 'target states' to separate the relevant infrastructures.

The rules prohibiting the infliction of unnecessary suffering or superfluous injury, enshrined in Article 35, are equally important, and yet equally problematic. Essentially the same features apply as above, and as with proportionality in its various guises, the external referent (i.e. the factor against which the necessity of suffering must be weighed[66]) remains the military utility of the end sought in the deployment of the 'method or means' under consideration.

Other rules of IHL, however, are considerably more determinate, not subject to external qualification, and are therefore far easier to apply. These would include the direct prohibition on attacks on civilians and civilian objects (e.g. the computer system of civil air traffic control) or objects indispensable to the survival of the civilian population (e.g. banks and financial institutions), the immunity of objects the destruction of which would release dangerous forces (an effective prohibition on attacks on the computer centres of Nuclear Power Stations), and the proscription on attacks against hospitals and medical personnel. In this regard, the benefits of considering SIW a use of force to be regulated by IHL are manifest.

However, the separation of infrastructures, and the devotion of governmental resources to the protection of its political/military infrastructures could have very unfortunate side effects in the absence of effective IHL regulation of SIW. Protecting a network from attack is a tricky, time-consuming, and hence expensive task.

> If you view our network like a building, like the Pentagon, [which] has hundreds of windows and doors in it, and I have to make sure that every single one of those doors and every single one of those windows is locked. An intruder only has to find one opening [...] To protect the virtual Pentagon, Defense Information Systems Agency staff spend their time trying to hack into it through the Internet, to identify the open windows [...] The defences [...] are constantly being breached."[67]

Obviously, once breached the defences are reassessed and improved, but a single, truly hostile, breach would constitute an attack in the fourth theatre of op-

65. *See* Higgins, *supra* note 57, para. 24.
66. *Id.*, para. 16; *See* Meyorwitz, *supra* note 55.
67. *See* The I-Bomb, *supra* note 2.

https://doi.org/10.1017/S0922156500000030 Published online by Cambridge University Press

eration; in this case the US interior. Such an attack could be launched from anywhere in the world, and could therefore prove an excellent countermeasure by a foreign power facing US forces on its own territory. The potential problems, and the need for IHL are thrust into relief when it is remembered that other (i.e. illegitimate civilian) targets will lack the protection afforded to the military nets, and will thus form potentially more tempting targets. This situation could easily be exacerbated by the removal of infrastructural interdependencies, and the consequent shared protections, demanded by IHL, as outlined above.

8. THOUGHTS FOR THE FUTURE

The impact on the *ius ad bellum* of a decision, or refusal, to define SIW as an armed attack must also be considered, as

> a modest but widespread attack could simply produce far larger consequences across the board due to poorly understood infrastructure interdependencies (e.g., between electric power and telecommunications) and catalyze an unexpectedly larger response and conflict escalation [...] Another complexity [...] is that some nations may develop SIW capabilities and hope that attacks with such weapons will only face responses in kind. However, there is no guarantee that an adversary nation will feel limited to an SIW response, especially if it has other instruments of [...] warfare readily available.[68]

While this seems obvious, it must be borne in mind that from a legal perspective, only a use of force, amounting to an armed attack, can countenance a legal resort to arms.[69] Therefore it would only be permissible to use force in response to an SIW attack if this could be considered as an armed attack. Although armed attack is nowhere defined in the UNC, and has been equated by others to an Act of Armed Aggression as defined by UNGA resolution on the Definition of Aggression[70] it would not seem beyond plausibility to consider SIW as an armed attack. As armed simply means using instruments to cause harm, and an attack is defined by Article 49 API as an "act of violence", the use of an alien program to disrupt a system could clearly be perceived as falling within this definition – all the more so when its (intended) effect is to cause injury or harm.

---

68. *See* Molander & Siang, *supra* note 8.
69. *See* Arts. 2(4) and 51 UNC; It should also be noted that the most recent definitions of armed conflict, given in the International Criminal Tribunal for the Former Yugoslavia in the *Tadić* case and approved by the chamber in the *Čelebići* case (para. 183) appear to view actual military force as a *sine qua non*. However, it is an open question as to whether such restrictive definitions spring from conceptual necessity, or simply follow from the circumstances of the all too apparent 'war' with which the Tribunal is concerned.
70. *See* McCoubrey &White, *supra* note 22, at 90. This betrays the general propensity to consider the intensity of a use of force, rather than analyse actions amounting to force, as the only relevant inquiry in defining an 'armed attack', i.e. separating this from use of force.

However, the designation of SIW as a use of force, capable of amounting to an armed attack, could also have serious consequences due to the fact that

> Potentially serious cyber attacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitred, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker.[71]

This could combine with a potentially wide, or at least widening, doctrine of anticipatory self-defence, to allow spurious claims of pre-emptive strikes to disguise aggression. Although it has been argued that "we delude ourselves if we think that the role of norms is to remove the possibility of abusive claims ever being made".[72]

It should be equally clear that the development of the law for the advancement of humanity should not serve as a tool for promoting or disguising breaches of fundamental prohibitions.

On balance, the classification of SIW as a use of force does more good than evil, and this is well illustrated by considering the consequences of failing to do so. Under the Friendly Relations Declaration[73] only reprisals involving the use of force are illegal. Thus, if SIW does not amount to a use of force (and therefore cannot be an armed attack), it cannot be responded to with conventional force, and the only viable retaliation would be in kind.[74] This could lead to the escalation to a full Strategic Information War (with the potential for grave suffering, death, etc) which would fall entirely outwith the regulation of IHL, and even of the Martens clause, and its "dictates of humanity".

If SIW is to be classified as a use of force, then recommendatory guidelines on the definition and separation of civilian and military computer infrastructures ought to be promulgated internationally, to provide clear concepts both of the substance of the duty not to use civilian shields, and the identification of military targets. On a related note, the concept and parameters of proportionality between responses – SIW to conventional; SIW to SIW; and conventional to SIW – will need to be elaborated.

The adaptability of such force to the domestic conflict paradigm would also merit consideration. Thus the point at which a hacker, or cracker,[75] would be deemed to use armed force (a difficult question given the threshold of violence

---

71. *See* PCCIP Paper, *supra* note 2.
72. R. Higgins, Problems and Process: International Law and How We Use It 247 (1994).
73. *See supra* note 35, UNGA Res. 2625 (1970), generally considered as customary international law, or, at least, as an authoritative interpretation of the UNC binding *qua* treaty.
74. However, Randelzhofer, in the Official Commentary to the UNC, does suggest that a military response to a non-military use of force could, under exceptional circumstances, be considered as a legitimate act of self-defence. *See* Randelzhofer, *supra* note 35, at 30. *See* also the Trial Chamber of the ICTY in its *Tadić* judgement, *supra* note 39, and accompanying text.
75. A hacker with criminal, or other evil, intent.

demanded by APII), and whether he would do so as a terrorist or a revolutionary, offer a sample of the issues such an adaptation could raise.

9. CONCLUSIONS

It would *prima facie* appear that SIW is at least potentially indiscriminate, as current infrastructural interdependencies make prediction of the consequences of an SIW attack all but impossible. Therefore determining whether these would be proportionate, a "feasible precaution" in attack as demanded by Article 58 API, does not appear viable. However, this is irrelevant unless SIW is regulated by IHL as it presently stands. Many specific rules of IHL appear appropriate to the regulation of SIW. Indiscriminate uses, and indeed SIW itself if these are inherent, would then be prohibited, even in the absence of a specific prohibition.[76] Therefore conscious efforts should be directed toward the explicit inclusion of SIW within the IHL/use of force paradigm *before* its omission, and consequently unregulated state, leads to serious humanitarian tragedy, and thus reaffirms the regrettably reactionary nature of IHL.

76. *See* I. Scobbie, *The Theorist as Judge: Hersch Lauterpacht's Concept of the International Judicial Function*, 5 EJIL 264, at 294-297 (1994). While a classic, or un-reconstructed, analysis of the *Lotus* presumption would allow the regulation or prohibition of a course of conduct only if a specific rule governed the area in question, this appears to have been based on a very common, misunderstanding or misreading of the case – or rather the context provided by the *compromis* on which it was decided, *see* Fitzmaurice (quoted *id.*, at 294). A truer analysis or re-floating of this idea, more in keeping with contemporary standards is offered by Dr Scobbie, who suggests using the presumption as a material rather than a formal mechanism of system closure. He thus advocates the analysis of rules and conduct in a systematised, and consequently non-atomised, manner. Under this approach, one need not find specific rules of prohibition, but can rather imply them from any substantive breaches of other rules which may be inherent in the given conduct.