Philos. Technol. (2015) 28:369–385
DOI 10.1007/s13347-014-0176-5

SPECIAL ISSUE

Violence, Just Cyber War and Information

Massimo Durante

Received: 27 March 2014 / Accepted: 2 October 2014 / Published online: 11 October 2014

Abstract Cyber warfare has changed the scenario of war from an empirical and a theoretical viewpoint. Cyber war is no longer based on physical violence only, but on military, political, economic and ideological strategies meant to exploit a state's informational resources. This means that a deeper understanding of what cyber war is requires us to adopt an informational approach. This approach may enable us to account for the two-dimensional nature of cyber war (destruction and exploitation), to revise the notion of violence on which war is premised and to understand to what extent the traditional ideas of 'just war' may apply to the scenario of cyber warfare. This point is crucial, since it concerns whether a cyber war is meant to restore a broken international political and legal order or to participate in its construction.

Keywords Cyber war · Information · Violence · Just war · Substantive rights

1 Introduction

War is a very old concept which has affected not only politics, law and history but also philosophy. War was meant to be the origin of all things (Heraclitus). The idea of becoming was seen as a conflict that marks the passage between being and not-being (Plato). The theoretical roots of war can be traced back to the idea of action, conceived as the capacity of an entity to affect another entity by destroying or modifying it. Thus, a war action has always had two dimensions: an act of destruction, which damages, deteriorates, deletes or suppresses an entity, and an act of exploitation, which alters, modifies or distorts an entity, in order to obtain something more or something different from what this entity is normally expected to be for.

The traditional view of war has changed from an empirical and a theoretical viewpoint. We progressively move from hard to soft powers (Nye 2004): in this scenario, the second dimension of a war action becomes more and more important. War is no longer based only or even mostly on physical kinetic armed attacks but also on political, economic, ideological and informational strategies intended to exploit

M. Durante (✉)
Department of Law, University of Turin, Turin, Italy
e-mail: massimo.durante@unito.it

someone else's informational resources. This does not amount to saying that war ceases to be destructive; rather, it means that a deeper comprehension of what war is in the cyber age requires us to take into full account these two dimensions.

'The impact of a cyber attack depends on what is targeted and more importantly what relies on that target' (Gervais 2011, p. 5). Cyber attacks target computers: our current information societies are everywhere increasingly based and dependent on computers. That is why a cyber attack is meant to be able to affect, either directly or indirectly, any trait of our societies, according to the unique (military) or dual-use (civilian and military) nature of targeted objects (Gervais 2011, p. 36; Richardson 2011, p. 27). That is also why it is so important to understand the conceptual core of a cyber attack, in order to better grasp its critical impact on our information societies.

2 The Twofold Informational Dimension of a Cyber Attack

The question arises as to what a kinetic cyber attack is: how force is to be interpreted in the cyber age. We need a unified approach to our understanding of a cyber attack, which may encompass the two dimensions of a cyber war: destruction and exploitation. Destruction is a traditional concept which belongs to the common representation of war, whereas exploitation is an area of rising importance fostered by the ongoing development of cyber war. A comprehensive theoretical framework is offered to us by the informational approach provided for by Luciano Floridi's philosophy (Floridi 2011) and ethics of information (Floridi 2013). This framework may enable us to deal with the conceptual core of the idea of cyber war, which is a war on information through information.

According to Floridi's philosophy of information, any entity is an informational object: 'any entity is a consistent packet of information, that is an item that contains no contradiction in itself and can be named or denoted in an information process' (Floridi 1999, p. 43). This is a static representation focused on the epistemological dimension of an informational object. On the basis of such representation, every epistemic subject can be an informational object at a certain level of abstraction. Some information entities are also agents, that is to say entities 'capable of producing information phenomena that can affect the infosphere' (Floridi 1999, p. 44). This means that an information agent is not only a consistent packet of information but also a source of information. This is morally relevant given that, according to Floridi's model of information ethics, an information agent can also be a moral agent in one of three ways, since she 'can avail herself of some information (information as a *resource*) to generate some other information (information as a *product*) and, in so doing, affect her information environment (information as a *target*)' (Floridi 2010, p. 102).

Some current definitions of cyber attack do not encompass some important aspects as the crucial dimension of exploitation. Three examples are the following (Gervais 2011, p. 8; Schimdt and Cohen 2013, p. 103):

> The damaging, deletion, deterioration, alteration or suppression of computer data without right', and 'the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating,

> altering or suppressing computer data. (Council of Europe, Convention on Cybercrime, opened for signature Nov. 23, 2001, 41 I.L.M. 282, articles 5–6)
>
> The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives (U.S. Army Cyber Operations and Cyber Terrorism Handbook, 2006, VII-2)
>
> Action by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption (Richard Clarke, former U.S. counterterrorism chief, cited in Schimdt and Cohen 2013, p. 103)

According to Gervais, even if cyber espionage or cyber exploitation is of greater importance as a major threat to commerce and national security, it 'fails to rise to the level of warfare', and 'does not violate the international laws of war' (Gervais 2011, p. 9). We do not want to stretch the concept of cyber attack, but we believe that consideration of cyber warfare should take into account its whole informational dimension (see for instance Hathaway et al. 2012, p. 821: "We […] describe three forms of cyber-attacks: distributed denial of service attacks, planting inaccurate information, and infiltration of a secure computer network" and Schmitt 2014, p. 21).

Other scholars speak of cyber intrusion when a broader concept is invoked (Kesan and Hayes 2012, pp. 439 and 440) and refer to cyber attacks and cyber exploitations to denote the two specific subtypes of cyber intrusions. A cyber attack is characterised by the fact that it seizes an entity as a 'source of information'. This may happen in two different ways (Floridi 2010):

- A cyber attack deprives an entity of its capacity to be *a* source of information because it damages, deteriorates, deletes or suppresses it. In these circumstances, a cyber attack is a disruptive activity, which patently rises to the level of warfare (for instance, when destroying or damaging a computing infrastructure).
- A cyber attack deprives an entity of its capacity to be *that* source of information it would have been if not under attack since it alters, modifies or distorts the way this entity is a source of information, or the information displayed by this entity (for instance, when intruding in an information system; when spying or torturing someone, to get strategic information). It may turn information into misinformation or disinformation (for instance, when disseminating false information through propaganda).

In these circumstances, which may encompass espionage or exploitation, a cyber attack is not a disruptive activity as such, but it can lead to disruptive effects which may rise to the level of warfare.

It is difficult to assess when a cyber attack amounts to a prohibited use of force under Article 2(4) of the United Nations Charter, for the very simple reason that 'force' is still interpreted as being traditionally associated with the military instrument. There are at least four approaches (Gervais 2011, pp. 11 and 12) to analysing force in cyber warfare:

1. The 'method of delivery', which takes into account the specific method of delivering an attack and prohibits cyber attacks based on how they are executed
2. The 'strict liability' model, which takes into account the specific target of an attack and prohibits cyber attacks directed against 'critical infrastructure'
3. The 'direct result' model, which takes into account the direct result of an attack and prohibits cyber attacks that attempt to cause direct physical destruction, injury or death
4. The 'consequence-based' model, which takes into account the reasonably foreseeable consequences of an attack and prohibits cyber attacks when their effect resembles that of a traditional attack

None of these approaches can account for all the aspects of cyber attacks, but each points out some issues that must be considered in order to have a full understanding of what is the recourse to force through cyber attacks. The following points are critical (Gervais 2011, pp. 11 and 12):

- Cyber weapons might be outdated by the time their prohibition is codified.
- The strict reference to critical infrastructure may collapse the distinction between armed violence, coercion and mere interference. A strict liability model would justify anticipatory self-defence in almost any case of a threat of harm aimed at a critical infrastructure.
- The direct effects of cyber attacks can result in non-physical damage.
- The indirect effects of cyber attacks may well result in physical damage that, therefore, should be taken into consideration, but it is often difficult to trace back the indirect effects to a specific cyber attack.
- It is hard to state whether the reasonably foreseeable consequences of a cyber attack resemble those of a conventional attack on the basis of six criteria (severity, immediacy, directness, invasiveness, measurability and presumptive legitimacy), which are not always applied and which account for the dynamics of cyber attacks. Which criterion prevails over the other? In such cases, there is 'little guidance as to the weight of each of the six factors' (Gervais 2011, p. 14) and the model leaves the way open for unconventional measures of coercion, like economic, diplomatic or ideological coercion (*ibid*, p. 15).

These points can be summed up by saying that the notion of cyber war is no longer based on conventional military instruments, physical damage, direct effect and strict armed violence. In this framework, we have to consider more closely how the idea of cyber war differs from that of conventional war. This requires us to investigate the idea of violence, which is of central importance across modern ages with regard not only to the concept of war but, first and foremost, to the idea of politics itself.

3 Cyber War and Traditional War

Cyber war changes the idea of war. Traditional war is mostly conducted by human beings through the use of physical force, namely, of kinetic violence. Traditional war is characterised both from a vertical and a horizontal viewpoint:

From a vertical viewpoint, traditional war is the sovereign state's claim addressed to its members, through which it calls them to be ready to sacrifice their life:

> When the prince says to him: 'It is expedient for the State that you should die,' he ought to die, because it is only on that condition that he has been living in security up to the present, and because his life is no longer a mere bounty of nature, but a gift made conditionally by the State. (Rousseau, ed. 1997, II.IV)

This places the essence of war in the conceptual framework of death. According to Hobbes, the modern sovereign state is constructed on and politically legitimated by its capacity to delay the individual's death: symmetrically, during wartime, such a delay is put off and the risk of death again becomes imminent.

From a horizontal viewpoint, war follows from a sovereign state's war declaration addressed to another state:

> War then is a relation, not between man and man, but between State and State, and individuals are enemies only accidentally, not as men, nor even as citizens, but as soldiers; not as members of their country, but as its defenders. Finally, each State can have for enemies only other States, and not men; for between things disparate in nature there can be no real relation. (Rousseau, ed. 1997, I.IV)

Declaration of war is essential to the traditional concept of war. Hobbes remarks that:

> For war, it consists not in battle only, or the act of fighting, but in a tract of time, wherein the will to contend by battle is sufficiently known; and therefore the notion of time is to be considered in the nature of war. (Hobbes ed. 2008, XIV)

According to Hobbes, war combines information and time: war is a tract of time, not in any chronological meaning, but rather as a form of anticipation based on the pending menace of battle and death, which therefore lies beneath both the vertical and the horizontal dimensions of traditional war.

In a globalised world, sovereign states' right to co-existence involves also a right and a duty to cooperate, based on their involuntary interdependence (Picone 1995, p. 519). Thus, the traditional concept of war changes, not only as a result of the evolution of cyber war but also as a result of the deep changes in the international context in which this concept has been elaborated. Globalisation, exacerbated by the digitisation that has turned sovereign states into computer-dependent societies, has gradually raised issues with the myth of sovereign states' self-sufficiency, the idea of an international legal order based on the equilibrium between isolated and autonomous sovereign states and the states' natural rights to act unilaterally, *uti universi* (Viola 2005, pp. 41 and 42).

The involuntary interdependence between sovereign states marks the shift from the traditional idea of government, based on the concept of will, to the contemporary idea of governance, based on the complexity of reality that transcends the idea of will. Such an involuntary interdependence generates also a tension that affects both national and international security.

3.1 National Security

At the level of national security, there is a strong tension between the principle of responsibility, according to which the authority entrusted with the responsibility to assure security also has the competence to decide what this security requires, and the duty to international cooperation, under which it is no longer feasible to guarantee national security without guaranteeing international security.

International security requires states to cooperate by setting up agreements and by providing these agreements with stability. We should not forget that, according to Hobbes, security is guaranteed by the stability of pacts. The societal immunisation from the imagined original violence is not meant to assure individual security but rather the stability of pacts; it is meant to assure individual security through the stability of pacts:

> The cause of fear, which makes such a covenant invalid, must be always something arising after the covenant made, as some new fact or other sign of the will not to perform, else it cannot make the covenant void. For that which could not hinder a man from promising ought not to be admitted as a hindrance of performing. (Hobbes, ed. 2008, XIV)

The stability of pacts depends on the available information already included in the hypothetical original violence, which enables us to anticipate 'something arising after the covenant [is] made, as some new fact or other sign of the will not to perform'. At the international level, there is, nonetheless, the problem of how to make agreements and have them respected without the use of force, since there is no international *Leviathan* and 'a covenant not to defend myself from force, by force, is always void' (Hobbes, ed. 2008, XIV).

3.2 International Security

There is a strong tension between sovereign states and the individual's claim to the protection of human rights in the international arena. There is a spreading tendency, furthered by digitisation, of individuals or groups of them to perceive themselves as international political subjects, both as patients, whose fundamental prerogatives are to be protected anywhere, and as single- or multi-agents willing to act on the international political scene. This raises the question of the state's responsibility for a distributed form of cyber attacks by non-state actors, which, if aggregated, may rise to the level of warfare.

4 Cyber War, Death and Peace

There are two more important changes with regard to cyber war. It is no longer only or primarily conducted by human beings (Pagallo 2011, 2013), and involving as it does information, it is no longer characterised by the Hobbesian relation between information and time. It is even difficult to state, in legal terms, when a cyber war begins and ends. In a pessimistic scenario, cyber war ceases to be a distinguished *tract of time*,

instead becoming an underlying constant stream of strategic operations. From this perspective, the idea of war, conceived as cyber war, no longer fits its modern conceptual framework: namely, the ideas of death and of peace.

4.1 The Idea of Death

This idea brings us back to the Hobbesian construct of modern political thought. Hobbes's great intuition is that the process of political legitimisation does not frame or solve the conflict but, rather, stems from it. If we want to capture what legitimises a political power, we have to realise from which conflict this power stems and to which conflict it is meant to be the answer.

When war is conceived in the theoretical framework of death, its legitimacy stems from two conflicts. Firstly, it originates from a horizontal conflict between sovereign states in the international arena and, secondly, from a vertical conflict between the sovereign state and its members who are called upon to potentially sacrifice their lives. Parliamentary authority to authorise war ultimate resides on this vertical conflict. Where war is no longer thought of in the theoretical framework of death because, for instance, it does not involve human combatants, its legitimisation ceases to be based on a vertical conflict. Rather, it is based solely on a horizontal conflict between states, which entrusts the process of war legitimisation to national government agencies. In this case, war is no longer considered and evaluated in relation to the primary value of human life, but becomes a matter of technological, economic, informational or other resources.

4.2 The Idea of Peace

The traditional concept of war is strongly linked to the concept of peace, and in many respects, it is at the foundation of this concept. The progressive transformation of the traditional concept of war in terms of cyber war is therefore also likely to affect the concept of peace. This is certainly of great importance, since the legal value of peace is or should be the basic principle of the international legal order.

The concept of peace is essentially procedural, tied up with the concept of war. From Hobbes to Kelsen (1966), peace is understood as the absence of war, that is to say, as the absence of the illegitimate use of physical force. The negative and procedural conception of peace tends to turn peace into security, from which it should be distinguished as it is in Article 2 of the Charter of the United Nations. This concept of peace seems to be inconsistent with the notion of cyber war, which does not require the use of force in the traditional sense. Bobbio (1979) describes peace in procedural terms, but less negatively, as the legally sanctioned conclusion of a war. This concept of peace can hardly be reconciled with cyber war, which does not necessarily have a legally sanctioned beginning and end (see the Stuxnet case: Richardson 2011 and, more generally, Kesan and Hayes 2012).

Thus, the concept of cyber war cannot easily be associated with the traditional idea of peace and it requires us to revise not only the traditional idea of war but also of peace, and hence the foundation of the international legal order. This revision goes far beyond the scope of this paper, but two issues are particularly important. The concept of cyber war is no longer conceived in the framework of death but rather of a

competition between different allocations of strategic resources. Secondly, cyber war is no longer thought of in the horizon of peace but of public security, which may be understood either in substantive (the factual conditions that enable sovereign states to have control over their life cycle of information) or in formal terms (the shared norms that govern the sovereign states' cooperation for the control over their life cycle of information).

We have insisted so far on the idea that cyber war differs from the traditional idea of war in that it does not necessarily make use of physical violence, although it may have indirect violent consequences. Physical violence thus marks a basic difference, at least in the premise, if not in the consequences, of kinetic and cyber attacks. However, the concept of violence is wider and more complex than the mere reference to the physical violence leads us to suppose.

5 The Modern Idea of Violence

In modern and contemporary political thought, violence is generally referred to and used as the theoretical foundation of the political order. Violence plays the role of a negative condition, from which a civil society is to be immunised in order to flourish as a stable and ordered political community. Violence is anthropologically founded: human beings are intrinsically violent, and violence is understood in kinetic terms as physical violence. This negative anthropology is already present in Luther and tends to characterise almost the whole tradition of modern natural law. The spark of physical violence is an energy that troubles the collectivity and needs to be controlled for the life of the political community to be possible. Two diverse ideas of violence originate here and find their theoretical formulation in Walter Benjamin's (1985) thesis on violence, which delineates the violence that *founds* the political order (including the law) from the violence that *preserves* it.

There is the idea that violence founds the existing political order. The original violence is to be immunised against: this allows the civil society to found a stable political order, which is then distinct from the premises from which it stems. Hence, the violence that arises from time to time is already included in the original violence, but is always of a lesser scale. The *imagining* of an original violence founding the political order turns out to be the unspoken justification of the existing political order, as magnificently accomplished in Hobbes.

There is also the idea that violence preserves the existing political order. The original violence is immunised against, but there is always a trace of it attached to the existing political order. The violence that arises from time to time is the undeletable trace of the original violence against which society cannot be completely immunised. The recourse to violence is what in the end assures the effective existence of that political order. The violence that preserves the existing political order proves that this order is never justified but is always potentially unjustified and inclined to make recourse to violence when necessary to reaffirm itself.

This genealogy of modern political order, justified and premised over the hypothesis of an original violence where this origin is not necessarily conceived in chronological or historical terms, is not based on a concept of violence exclusively understood in terms of physical violence. Let us delineate two diverse forms of violence, concerned

with its means and ends. The means of violence concern how violence is perpetrated. There are, naturally, many ways to manifest and accomplish violence, which are not limited to physical force. Verbal or psychological violence, for instance, does not require recourse to physical force, although the primary and basic manner to be violent is by means of physical force. Therefore, we define this form of violence as physical violence.

The ends of violence are different from how it is manifested and accomplished. Although there are exceptions (for instance, blind violence or the so-called systemic violence; Žižek 2008), violence is generally meant to achieve something that goes beyond its manifestation. Thus, we define this form of violence as moral violence. We do not take moral to refer to anything ethically justified but rather to an end not immediately perceivable in the manifestation of violence.

Throughout history, the idea of physical violence has been always coupled with the idea of moral violence, which plays a key, yet less visible, role in the foundation of the political order and in the justification of war. In some cases, the use or the impediment of physical violence is justified as far as it prevents moral violence. In other cases, the use or the impediment of moral violence is justified insofar as it stops physical violence. In this sense, physical and moral violence function as two normative systems that can be engaged or disengaged in order to serve as a justification for each other (for the relation between violence and morality, see Magnani 2011; for a commentary, see Durante 2013).

Let us sketch the interplay of physical and moral violence in Hobbes' and Locke's political philosophies, where this interplay underlies both the construction of their social contract theories and the conceptual relation between the state of nature and the state of war.

Unlike Hobbes, Locke makes a distinction between the state of nature and that of war. The Lockean state of nature is the state in which human beings live together according to reason, without a common superior with authority to judge between them. The state of nature is not characterised by the war of all against all (that is, by physical violence) but by the lack of a common judge to appeal to. This lack opens the way of getting justice ourselves, which is justified as the law of war when it comes to reject those who want to deprive us of freedom, or is unjustified when it conceals the use of force without right. The state of war is characterised by recourse to force or by its menace, when there is not a common superior to appeal to or when force is exerted without right, even if in the presence of a common judge:

> Want of a common judge with authority, puts all men in a State of Nature: force without right, upon a man's person, makes a State of War, both where there is, and is not, a common judge. (Locke, ed. 1998, 3.19)

Locke goes on

> The law, which was made for my preservation, where it cannot interpose to secure my life from present force, which, if lost, is capable of no reparation, permits me my own defence, and the right of war, a liberty to kill the aggressor, because the aggressor allows not time to appeal to our common judge, nor the decision of the law, for remedy in a case where the mischief may be irreparable. (Locke, ed. 1998, 3.19)

Again, morality consists in introducing a delay in the immediateness of life. Here, Locke introduces a different concept of violence, which concerns moral violence. It is apparent that, according to Locke, violence is primarily moral violence, which consists of getting justice by itself (being the judge in our own case) through the use of force without right. Self-defence is justified and even required when the subject of aggression is in the absence of a common judge. The moral foundation of Locke's political philosophy is the delegation of justice—the appeal to a common superior. According to Hobbes, security may be achieved only through the stability of pacts and moral violence consists of the betrayal of pacts:

> Thus the nature of justice consists in maintaining the valid covenants, but the validity of the agreements will not start if not with the constitution of a civil power sufficient to compel men to keep them. (Hobbes, ed. 2008, XIV)

The stability of pacts is promoted by the common interest to escape from the state of nature dominated by physical violence and guaranteed by a civil power that compels people to maintain valid covenants. It is the fear of physical violence that leads us to overcome the risk of moral violence.

According to Locke, security may be achieved only through the delegation of justice, which draws the distinction between the state of nature (moral violence: lack of a common judge) and that of war (physical violence: fear of death). We can free ourselves from physical violence only by overcoming moral violence. In the Lockean state of war, there is no appeal: 'war is made upon the sufferers, who having no appeal on earth to right them, they are left to the only remedy in such cases, an appeal to heaven' (Locke, ed. 1998, 3.20); 'where there is no judge on earth, the appeal lies to God in heaven' (Locke, ed. 1998, 3.21).

Physical violence is always coupled with moral violence. According to Hobbes, physical violence conceptually underlies moral violence: it is the disengagement from physical violence that assures the maintenance of pacts. According to Locke, moral violence conceptually underlies physical violence: it is the disengagement from moral violence that frees human beings from the threat of physical violence. Physical and moral violence are dissimilar, but they have a common conceptual ground that allows us to define the essence of violence. Let us state it by referring to what Emmanuel Levinas has pointed out (for comments, see Durante 2003):

> Violence is to be found in any action in which one acts as if one were alone to act: as if the rest of the universe were there only to receive the action: violence is consequently also any action which we endure without at every point collaborating in it. (Levinas 1990, p. 6)

Hence, violence is what turns an agent into a mere patient or what prevents a patient from becoming an agent. Violence is found in any action in which one acts regardless of another member or instance of the universe. The conceptual core or the essence of violence is its radical *regardlessness*. This also traces the limit one should never trespass when justifying the recourse to violence. Physical violence is never justified as such, but only by juxtaposing it with a moral violence to be avoided. In this sense, the use of force requires a moral engagement or, in the vocabulary of the just war

tradition, a *iusta causa*, namely, a 'good reason'. We should then focus on the possible justifications of war, that is, on the tradition of just war (*Jus ad bellum*).

6 Two Theories of 'Just War'

Traditional theories of just war are mainly centred on the interpretation of what is the *iusta causa* (the good reason) for war (Viola 2005, p. 55). There is no space in this paper to account for all just war theories, but let us follow Francesco Viola (2005, pp. 56–60), who discerns two traditional interpretations of just war.

6.1 The School of Natural Law and the Modern *Ius Gentium*

According to the School of Natural Law and to the modern *Ius Gentium* (Grotius etc.), the *iusta causa* resides in the right to self-defence from aggression. As seen in Locke, all human beings and nation states have the natural right to self-defence, 'because the aggressor allows not time to appeal to our common judge, nor the decision of the law, for remedy in a case where the mischief may be irreparable' (Locke, ed. 1998, 3.19). This is taken for granted by Vitoria, Suarez and Grotius and is not subject to dispute. What is under discussion is the extent of the class of rights (goods or values), which authorise the state's reaction against the aggressor (Viola 2005, pp. 57 and 58). Life and freedom are naturally included, but property, for instance, is under debate, as are the controversial limits of the state's reaction: *Jus in bello*. What is common to all scholars, until Hobbes, is that self-defence is allowed only against the tangible threat of an imminent danger. It is Hobbes that introduces the idea (consistent with the essential role that imagination plays in his political philosophy: see chap. II–III of *Leviathan*) that self-defence can be preventive: that is to say, based on the supposed menace of a potential danger. It is a central, striking idea affecting the whole development of the notion of Just War. With regard to this preventive attitude, Hobbes formulates what we might consider the first account of what cyber war is and requires from those that govern:

> Since therefore it necessarily belongs to rulers for the subjects safety to discover the enemies counsels, to keep garrisons, and to have money in continual readiness, and that princes are by the Law of Nature bound to use their whole endeavour in procuring the welfare of their subjects, it follows, that it is not only lawful for them to send out spies, to maintain soldiers, to build forts, and to require money for these purposes, but also, not to do this, is unlawful. To which also may be added, whatsoever shall seem to conduce to the lessening of the power of foreigners whom they suspect, whether by sleight, or force. For rulers are bound according to their power to prevent the evils they suspect, lest peradventure they may happen through their negligence. (Hobbes, ed. 1998, XIII, 8).

This preventive attitude (which includes three basic informational strategies: discovering the enemies' intents, lessening their powers by sleight and preventing their suspected evils) is of key importance, since prevention is not directed to restore a broken political international order but rather to take part in its construction. A 'just

cyber war' is thus characterised not only by a defensive or reactive role but, first and foremost, by an active or constructive one. This preventive attitude can become the most important side of cyber war. Would this mean that some forms of cyber war will be normalised and included in states' political strategies in international relations? Is preventive cyber war going to be a form of distributed control, at the international level, on strategic life cycles of information, namely a form of control concerned with the discovery of intent, the lessening of powers and the prevention of evils? Our idea is that cyber war will not simply take the place of traditional war in many cases as a form of continuation of politics by other means. Cyber war, understood as exploitation rather than destruction, will be a steady and significant part of current international politics.

6.2 Middle Age Tradition

According to a different tradition going back to St. Thomas and St. Augustine, the *iusta causa* resides in the protection of the weak and the oppressed. In this sense, just war is not motivated by self-defence but by the need to protect someone else and to punish the aggressors for their faults. According to St Thomas, the justification of just war is not defence but the protection of common good. St. Thomas does not treat the issue of war as part of natural law or justice but in relation to the virtue of charity: 'he does not wonder whether a war is moral, but whether it is always sinful to make a war, namely, in what case to kill another human being is not contrary to the love for the neighbour' (Viola 2005, p. 60). Viola remarks that the protection of common good, which authorises a just war, concerns:

> …both those who are to be protected and those who are unjustified aggressors. In fact, a just war is made in support of other people as well as in the interest of the enemies themselves. Thus, all the hypotheses envisaged by St Thomas concern the use of war as a sanction, which is intended to punish a fault and to fulfil the claims of justice. The recourse to war has to be premised upon a very serious injustice to be punished, as in the case in which a State does not sanction the violence perpetrated by its members or does not return what unlawfully obtained. (Viola 2005, pp. 59 and 60)

War is thus justified when it comes to redress someone else's unjust sufferings (*Jus ad bellum*), and this is done in a proportionate manner (*Jus in bello*). This interpretation of just war is not limited to the hypothesis of self-defence but is primarily concerned with someone else's unjust sufferings, and thus, it may embrace the protection of human rights. Viola remarks that 'it is with this middle-age tradition that we have to be deal, since it is more apt to interpret the current claims of just peace than the modern tradition is' (Viola 2005, p. 60). This interpretation implies a clear understanding of the causes of injustice that authorise a war: namely, we need to share a list of values (constitutional principles, human rights, fundamental goods) the infringement of which makes someone else suffer from unjust causes that ask for intervention at the international level. In this framework, just war is intended to restore a broken international political order on the basis of recognised shared values. In this respect, we have to make two critical remarks.

6.3 Pluralism

It is hotly debated whether the recognition of a comprehensive list of values is possible when confronted with a pluralistic conception of human rights and to what extent values, if recognised, are shared. These are difficult questions with issues of pluralism and universalism and cannot be dealt with in pure theoretical terms. The use of legitimate force can be justified on moral grounds, but these are more concerned with the practical impediment to moral violence than with the identification of what is just. Thus, the question is, What is moral violence in the cyber age? Is it the infringement of pacts, as global interdependence raises a duty to trustful cooperation, or the lack of appeal to a common superior? We argue, in the last part of the paper, that the answer depends on a full appraisal of the informational nature of cyber war.

6.4 Preventive War

A just war attack can be preventive when directed to the defence of the weak or the oppressed, and it is hardly arguable that the intervention is intended only to restore the broken political international order. A preventive intervention seems always aimed at participating in the construction of that order. The preventive intervention also has to show the moral grounds on which the reason to intervene rests, which differ from national interests and security reasons. Such reasons mainly refer to the protection of the public internal order of the international community.

7 Just Cyber War

Let us rehearse what we have said so far. Cyber war changes the notion of war dramatically, and this change also affects the idea of a possible just cyber war. This change is due to the fact that cyber war is hardly related to the traditional legal ideas of peace, either the procedural and negative idea of peace as the absence of illegitimate violence or the procedural and positive idea of peace, according to which peace is the legally sanctioned conclusion of a war. In this perspective, cyber war is not understood as a declared conflict between sovereign states, finally directed to re-establish peace, by re-assuring control over a territory and hence national (or international) security. On the contrary, cyber war is conceived as an undeclared conflict and tactical competition between national agencies which is directed to reassure national or international security by having control over strategic flows of information. Against this backdrop, cyber war is less aimed at restoring a broken international order than at participating in its construction. Cyber war has thus a proactive rather than a merely reactive nature. This is consistent with the structure of the Information Society, which is increasingly an inference society, based on the pre-emptive capacity to anticipate future trends and behaviours.

Therefore, contrary to the emphasis placed at present on human rights that supports the idea of ‘just peace’ (Viola 2005, p. 60), we believe that a just cyber war is meant to mostly endorse the Hobbesian tradition of preventive self-defence. Just cyber war is hence characterised by a proactive, constructive role, because of which it becomes more and more a preventive form of control, at the international level, over strategic life

cycles of information. Since Hobbes, this form of control includes three key informational strategies: (a) the discovery of enemies' intents, (b) the lessening of their powers by means of sleight and (c) the prevention of their suspected evils. All these activities are mainly based, as remarked, on the element of covertness:

> The element of covertness is a tricky area of international lawyers. It is an emerging area that will gain great resonance at state increasingly turn to covert cyber attacks to achieve their goals. There is no bright-line rule on whether a covert cyber attack will be held unlawful by the international community for the reason of its covertness; whether a covert cyber attack is held unlawful depends on any number of contextual factors. (Gervais 2011, p. 31)

In the Hobbesian perspective, moral violence is overcome when pacts are stable and respected. In the absence of a superior power that compels states to respect the pacts, the stability of pacts depends on available information which enables states to predict whether there is 'something arising after the covenant made, as some new fact or other sign of the will not to perform' (Hobbes, ed. 2008, XIV). Therefore, moral violence is mainly concerned with tightening international collaboration between states.

The duty of collaboration arises from mutual interdependence and the need to cope with the distributed nature of cyber attacks, mainly perpetrated by non-state actors. The duty of collaboration is directed at assuring that (a) states adopt reasonable measures to prevent foreseeable cyber attacks from non-state actors that originate from its territory (Gervais 2011, p. 20); (b) states adopt reasonable measures to discontinue (or make reparations for) the wrongful conduct of non-state actors that originate from its territory, when a series of incidents cannot be considered in isolation but, according to an accumulation doctrine, as a single armed attack; (c) states are accountable for the dangers of covertness of cyber attacks, which '*can* transform an otherwise lawful operation into an unlawful action under international law' (Gervais 2011, p. 29); and (d) states provide other states with a sufficient level of information, in order to make them discriminate between combatants and civilians: this is more difficult to achieve when cyber attacks are run by non-state actors.

These cases are all concerned with the quantity and quality of information shared, or with data in any way gathered, which enable us to make predictions about future trends and behaviours. Cyber war is not only conceived in informational terms but is a war on information through information. Let us consider more closely the informational nature of cyber war and the idea of informational moral violence. This may help us determine whether a cyber war is justified only in case of self-defence or also for the protection of human rights (i.e. in support of the weak and the oppressed).

The main difficulty in justifying the use of force for the protection of human rights resides in their pretended universality, as Viola puts it:

> The assertion of their universality often conceals the belief in the superiority of the western conception of human rights based on individualist philosophy, which is neither accepted nor shared by different cultures, notably, the oriental ones, more sensitive to communitarian values and collective rights (*Asian values*). Therefore, a war justified by the need to protect human rights would be easily

> used to impose the supremacy of western values and of the political and economic systems related to them. (Viola 2005, p. 61)

There is a possible reply to this argument. Not all human rights should be used to justify the recourse to force (Viola 2005, p. 61). There is a limited number of fundamental rights which are so necessary that they enable the exercise of all the others (Shue 1980, cited in Viola 2005, p. 62). Any type of rights, whether liberal or communitarian, individualistic or collectivistic, is premised upon such fundamental rights:

> These rights have been defined as socially basic human rights: their respect is the minimal condition for human dignity. Certainly, they include security, that is, the right not be killed, tortured or aggressed (*security rights*), and the rights to subsistence (*subsistence rights*), namely, the right to adequate food, clothes, housing as well as clean air and water. It is debated whether negative freedom should also be included among these elementary rights, as I believe. One might assume that all human beings, despite their cultural identity and particular theory of rights, should agree on the fact that being deprived of one of these fundamental rights is considered a serious violation of human dignity. This may be judged, under certain conditions, a good reason for war. (Viola 2005, p. 62)

Let us consider what is, in informational terms, a deprivation of fundamental rights that amounts to a serious violation of human dignity. This brings us back to the issue of what constitutes moral violence from an informational standpoint. It is obvious that physical violence is accomplished when a disruptive activity damages, deteriorates, deletes or suppresses an informational object. In this case, the entity seized by the violence ceases to be an informational object. This entity is no longer a source of information. The protection of the mere existence of an entity as a source of information is part of its security rights, that is, the right not to be destroyed or aggressed. When is moral violence then perpetrated?

Violence is found in any action in which one acts regardless of any other member or instance of the universe. The essence of violence is thus its radical *regardlessness*. Violence is what turns an agent into a mere patient or what prevents a patient from becoming an agent. A patient is, thereby, deprived of the fundamental capacity to become an agent and, hence, to become a *specific* source of information. A violent act prevents an entity from becoming *that* source of information which it could have been had it not been subject to violence. For this reason, an information agent can no longer be a moral agent, since she cannot 'avail herself of some information (information as a *resource*) to generate some other information (information as a *product*) and, in so doing, affect her information environment (information as a *target*)' (Floridi 2010, p. 102). From an informational standpoint, moral violence is the deprivation of such key capacity: i.e. to be *that* specific source of information.

The deprivation of this capacity is part of the security rights of an informational agent, when it concerns its right not to be tortured (i.e. the right not to be *that* source of information it would not have been if not subject to violence), and so *vim vi repellere licet*; the impediment of informational physical or moral violence authorises the recourse to force. Informational security rights are part of the *socially basic human*

rights that justify a cyber attack. The basic questions are, therefore, whether or not to be *that* source of information may as well count as a *subsistence right*, and can the deprivation of informational subsistence rights authorise the recourse to force? The answer is to be found in the nature itself of affordances of subsistence rights. A subsistence right is considered a social basic human right, the disrespect of which is a serious violation of human dignity authorising the recourse to force, when it affords the possibility to exercise all the other human rights, whether liberal or communitarian, individualistic or collectivistic. Therefore, a specific source of information counts as an informational subsistence right, when it affords the possibility to exercise all the other rights. In this case, the protection of *that* source of information is a legitimate reason for war. The informational approach may have a further consequence. Being a specific source of information allows the agent to be what it is as a moral agent, and thus, the informational subsistence right coincides also with negative liberty, if this is conceived as the necessary requirement for moral choice and human flourishing. This means that the informational approach widens the scope of subsistence rights, by including negative liberty within the socially basic rights that authorise the intervention to protect the weak or the oppressed.

8 Conclusions

This informational approach accounts both for the case of cyber destruction, which is meant to deprive an entity of its capacity to be *a* source of information, and for the case of cyber exploitation, which is meant to deprive an entity of its capacity to be *that* source of information it would have been if not attacked. Aware of the lesson of modernity, it couples physical violence with moral violence and provides us with some hints about what form of cyber attacks may be considered justified. It also tells us that, in the long run, the informational nature of cyber war will turn war into a strategic competition between national agencies for the control over the life cycle of information at the international level. This warlike competition will not be a continuation of politics by other means but part of current international politics. Finally, the informational approach suggests to us that cyber war will inherit from the Hobbesian tradition a preventive attitude towards self-defence which is directed to participate in the construction of the international legal order. Since cyber war is no longer 'a tract of time' but something progressively displaying in covert areas, this will raise questions of transparency and accountability. Nonetheless, the violation of informational security and subsistence rights will authorise recourse to force to protect the weak and the oppressed. To what extent and in what circumstances the protection of informational security and subsistence rights will be considered a legitimate reason for war is left to future investigation.

References

Benjamin, W. (1985). *Critique of violence [1921], in one-way street, and other writings* (pp. 132–154). London: Verso.

Bobbio, N. (1979). *Il problema della guerra e le vie della pace*. Bologna: Il Mulino.

Durante, M. (2003). *Violenza e diritto nella riflessione d'Emmanuel Levinas. Riflessioni sul post-totalitarismo*. in AA. VV. Annali della Facoltà di Giurisprudenza dell'Università di Ferrara, Nuova Serie, Vol. XVII, Giuffré, Milano, 141–164.

Durante, M. (2013). Notes on Lorenzo Magnani understanding violence. *Mind & Society, 12*(2), 257–262.
Floridi, L. (1999). Information ethics: on the philosophical foundation of computer ethics. *Ethics and Information Technology, 1*, 37–56.
Floridi, L. (2010). *Information. A very short introduction*. Oxford: Oxford University Press.
Floridi, L. (2011). *The philosophy of information*. Oxford: Oxford University Press.
Floridi, L. (2013). *The ethics of information*. Oxford: Oxford University Press.
Gervais, M. (2011). *Cyber attacks and the laws of war (October 1, 2011)*. Http://ssrn.com/abstract=1939615.
Hathaway, O.-A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review, 100*, 817–885.
Hobbes, T. (Ed.). (1998). *De Cive [1642]*. Cambridge: Cambridge University Press.
Hobbes, T. (Ed.). (2008). *Leviathan [1651]*. Oxford: Oxford University Press.
Kelsen, H. (1966). *Principles of international law* (IIth ed.). New York: Holt, Rinehart and Winston.
Kesan, J. P., & Hayes, C. M. (2012). Mitigative counterstriking: self-defence and deterrence in cyberspace. *Harvard Journal of Law& Technology, 25*(2), 429–543.
Levinas, E. (1990). *Difficult freedom. Essays on Judaism*. London: The Athlone Press.
Locke, J. (Ed.). (1998). *Two treatises of government [1690]*. Cambridge: Cambridge University Press.
Magnani, L. (2011). *Understanding violence. The intertwining of morality, religion and violence: a philosophical stance*. Berlin-Heidelberg: Springer.
Nye, J.-S. (2004). *Soft powers: the means to success in world politics*. New York: Public Affairs.
Pagallo, U. (2011). Robots of just war: a legal perspective. *Philosophy and Technology, 24*(3), 307–323.
Pagallo, U. (2013). *The laws of robots: crimes, contracts, and torts*. Dordrecht: Springer.
Picone, P. (1995). Interventi delle Nazioni Unite e obblighi *erga omnes*', in Id. (a cura di). *Interventi delle Nazioni Unite e diritto internazionale,* Cedam, Padova.
Richardson, J.-C. (2011). Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield (July 22, 2011). Http://ssrn.com/abstract=1892888.
Rousseau, J.-J. (Ed.). (1997). *The social contract [1762]*. Cambridge: Cambridge University Press.
Schimdt, E., & Cohen, J. (2013). *The new digital age: reshaping the future of people*. Knopf: Nations and Business.
Schmitt, M.-N. (2014). The law of cyber warfare: quo vadis? in *Stanford Law and Policy Review*. forthcoming, 1–24.
Shue, H. (1980). *Basic rights: subsistence, affluence, and U.S. foreign policy*. Princeton: Princeton University Press.
Viola, F. (2005). La teoria della guerra giusta e i diritti umani, in AA.VV., *Pace, sicurezza, diritti umani,* a cura di S. Semplici, Messaggero, Padova, 39–68.
Žižek, S. (2008). *Violence*. London: Profile.