ISSN: 1825-5167

ETERNAL HOBBES: INTERNATIONAL RELATIONS AND CYBERWAR

PIERPAOLO MARRONE
Università di Trieste
Dipartimento di Studi Umanistici
marrone@units.it

ABSTRACT

Is the Hobbesian state of nature a valid paradigm for international relations between states? Starting from the territory of ICT ((Information and Communication Technologies), this paper explores some issues related to cyberwar and cyberspace and their implications for international relations. My conclusion is that there are good reasons to be sceptical about the very existence of international law, just because this explanatory paradigm should also apply to this area.

KEYWORDS

Hobbes, international law, war, sovereignty.

1. In the Hobbesian paradigm, what is not forbidden by the sovereign is within the citizen's availability for action. Sovereignty is a willingness to control bodies for the purpose of collective security. This collective security coincides for Hobbes with the absence of faction, that is, with the absence of seditious groups that do not recognise the absolute authority of the sovereign, but place it in something else, beyond sovereignty. For Hobbes, who had known the disaster of religious wars, this meant that positive law was the only existing law, outside of which it was simply not possible to recognise any right except that of the *jus ad omnia*, which is the structurally permanent prodrome of civil war, the greatest of evils. However, if outwardly citizens must obey the orders of the sovereign, who guarantees the security of their life's enjoyment, inwardly they can cultivate the beliefs that best suit their life plans, which citizens can translate into action plans, if these are not explicitly forbidden by the sovereign. It can be argued, without great straining, that this paradigm is both a foundation of positive law through absolute sovereignty, i.e. without transcendent constraint, and the foundation of a right to what we might call the privacy of the individual.

Another consequence of the Hobbesian conception of sovereignty is that while it guarantees the exit from the state of nature through the emergence of the state that coincides with civil society, it re-proposes this same state of nature in international relations, where there is no sovereignty, but the potential war of antagonistic sovereignties. From this factual consideration, the non-existence of a world sovereign, some have drawn the conclusion that to speak of international law is a contradiction in terms, when the very fact of the existence of a multiplicity of sovereign states belies the absolute dimension of sovereignty. Some clarifications must be made on this point. If by international law is meant a law such as the internal positive law of the state, which can be imposed through the state's monopoly of coercion, then international law obviously does not exist. There is, however, apparently a weaker way of understanding the existence of international law, such as the agreement between two or more states that sign treaties that have the force of law and that rely on arbitrators, who may possibly dispense sanctions, in the event of disputes. This is why we speak of European Union Law, for example. It is clear that this is something different from the positive law of the state that holds the monopoly of coercion, because it is not clear what could happen in the case of a dispute between states where one of the defendants refuses to implement the sanctions that had been decided against them by a third-party arbitration. Unless the arbitrator has an international army or police force, it is difficult to see how international law can be enforced. One of the examples given to support the existence of international law is that of the International Criminal Court. This is an unfortunate example, however, because the United States, China, Russia and other states are not members of this criminal court. International Criminal Court is therefore unable to prosecute any crimes that are committed in the territories of these states. The idea that has sometimes emerged in the public debate in recent months of dragging Putin before the International Criminal Court is therefore at the moment completely unrealistic, and this converges with the opinion of those who argue that international law does not exist. But there are also other reasons to question the existence of the effectivity of international law, which I will explore in the following pages in relation to new cybernetic technologies.

2. The war that is infesting Europe at the moment has both all the features of a traditional conflict (troop movements on the ground, supply lines, stochastic bombing, war for domination of the skies, naval attacks, disinformation techniques)[1] and the characteristics of a conflict where information infrastructures have a significant, though difficult to assess weight.

War is of course the moment that exalts the Hobbesian intuition of the potentially permanent conflict in the human community. Hobbes' idea was that, if the state of nature could be neutralised thanks to the invention of sovereignty, that is, thanks to the permanence of what we still call the State, it would be very difficult

[1] E. Di Rienzo, *Il conflitto russo-ucraino. Geopolitica del nuovo (dis)ordine mondiale*, Rubettino, Soveria Mannelli, 2015, for an examination of the antecedents of this conflict in terms of political realism; L. Caracciolo, *La pace è finita*, Feltrinelli, 2023.

to do so at the level of relations between States, which would continue to be governed not by the invention of law and the exercise of legitimate coercion, but by force.[2] Some even doubt that international law exists, since there is no sovereign capable of applying it; others are highly sceptical about its possibility of applying it in general regardless of specific contexts. [3]

I will explore in these pages some suggestions that might support Hobbes' idea of the permanence of the state of nature in international situations involving relations between States. I will do so by trying to balance some intuitions, supported however by the literature, on the so-called *cyberwar*.[4] It must be said that the positions on this new terrain of confrontation between military powers are by no means uniform. Roughly speaking, it can be argued that there are those who believe that *cyberwar* techniques do not exclude recourse to instruments of control under international law, and those who believe that even in this case international law is a fiction ready to collapse at the first hint of real, and not just virtual, war. [5]

Cyberwar techniques include selective attacks on adversaries' computer systems, massive stochastic attacks that prepare the field for subsequent targeted attacks, election propaganda in a foreign country to favour certain candidates and harm others, industrial espionage, and interference in civilian computer infrastructures such as tax databases, health databases, electricity grids, and transport systems. These techniques have triggered an escalation of data protection systems, to which, of course, software that breaks through these systems has responded. This escalation is also accepted as normal by the public, which has generally formed the opinion that there is no software system or database that cannot be hacked.

According to popular literature, TV series and movies, it would be enough to have access to the Internet and the necessary technical skills that could be acquired even by *nerdy* teenagers barely above the threshold of sociopathic disorders. Software from potentially hostile countries, such as the famous Kaspersky anti-virus, is also being scrutinised in these days of raging war between Ukraine and Russia to see if it contains dormant *worms* that can be activated at the right time.

Telephone companies such as Huawei, capable of creating infrastructure for entire nations (including the laying of important submarine cables), are being

[2] T. Hobbes, *Leviathan* (1651), Rizzoli, Milan, 2011.

[3] M. Koskenntemi, *The Gentle Civilizer, The Rise and Fall of International Law,* Cambridge University Press, Cambridge 2001, for a history and critique of international law; D. Zolo, *I signori della pace. Per una critica del globalismo giuridico*, Carocci, Rome, 2001, for a conflictual view of international relations and their codification in international law.

[4] For a first approach A. Bonfanti, *Attacchi cibernetici e cyber war: Considerazioni di diritto internazionale*, in "Notizie di Politeia", XXXIV, 132, 2018, pp. 118-127; M. Durante, *Violence, Just Cyber War and Information*, in "Philosophy & Technology", XXVIII, 3, 2015, pp. 369-385; B. Romaya, L. Portmess, *Confronting Cyber Warfare: Rethinking the Ethics of Cyber War*, in "The Journal for Peace and Justice Studies", XXIII, 1, 2013, pp. 44-60

[5] R. Dipert, *The Ethics of Cyberwarfare*, in “Journal of Military Ethics”, IX, 4, 2010, pp. 384-410 for a comparison of these two positions.

banned by Western countries, since they are categorized as China's instruments in the fight for world hegemony.[6] These are just a few of the facts that have recently reached a public dimension, which contribute to drawing a picture of a world dominated by cyber-anarchy, always on the brink of disastrous implications for financial, economic, and geo-strategic equilibria. These facts cast serious doubts on the capacity of democracies to deal with threats of this new kind, since democracies imply by their very nature the presence of political systems built on the division of powers and on systems of checks and balances with dilated decision-making times. These extended decision-making times are ill-suited to this new kind of threat, which can develop in a matter of minutes or even seconds.

3. The idea of implementing mandatory rules for cyberspace has generated many perplexities. There is not only the fact that a *super partes* authority, i.e. above the States, does not appear to be identifiable at the moment, but to this, should be added the issue that no state has actually declared to voluntarily renounce the competitive advantages that are, even only momentarily, generated by a tactical superiority in potential cyber attacks against enemy countries.

There has certainly been no lack of attempts in this direction. For instance, the United Nations Organisation has, under pressure from the Russian Federation, been discussing "Developments in the Field of Information and Telecommunications in the Context of International Security" since 1998,[7] as the title of the resolution approved at the time states, which should have led to the adoption of stringent security standards in the field of ICT (Information and Communication Technologies) in the event of war. Switzerland has implemented a package of principles for the responsible behaviour of States in cyber space, which are derived from numerous discussions in various international forum and which were approved by the UN.[8]

These are:

(1) Foster inter-state cooperation in the field of cyber security;

(2) Consider all relevant information;

(3) Prevent the misuse of ICTs in their territory;

(4) Enhancing inter-state cooperation to prevent and suppress criminal activities in cyber space;

(5) Respect the human rights and privacy of citizens;

(6) Not to damage critical infrastructure of other States;

(7) Protect its own critical infrastructure;

(8) Respond to requests for assistance from other States;

[6] Yun Wen, *The Huawei Model: The Rise of China's Technology Giant*, University of Illinois Press, Champaign, 2020.

[7] https://www.un.org/disarmament/ict-security/

[8] https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html

(9) Ensuring supply chain security for ICT networks;

(10) Publicly report on ICT vulnerabilities;

(11) Not to damage the teams responding to computer emergency requests.

It is easy to see that these are essentially principles of goodwill and by no means strict rules. Their very vagueness heralds the possibility only of further statements of principle, rather than sufficiently precise rules. Let us take the statement in (2) that all relevant information must be considered. The very concept of 'relevant information' is completely ambiguous,[9] because one piece of information may be relevant only at a later, indefinite time with respect to the present, whereas another piece of information may be considered relevant and not be relevant at all.

This interpretative ambiguity may be more of a tool for not sharing information than for sharing it. As for the statement in (5), this seems to refer to the various charters of rights approved by international bodies.[10] There are, however, so many documented cases of violations of these rights by nations that have signed up to them, that the nature of the statement of good intentions is evident even here. Moreover, it must be added that some nations are not at all in agreement on the content of individual human rights.

China, for example, has always declared that these must be declined within its conception of human rights, where individual rights are subordinated to the collective welfare of larger entities (basically the Chinese Communist Party and its role in contemporary China).[11] Moreover, it is well known that the conception of privacy, while it has undergone an important evolution even in democratic countries, has a completely different meaning in countries ruled by dictatorships or otherwise authoritarian systems.[12] With regard to the principle stated in (6), the Russian Federation itself, which is one of the countries at the origin of these noble statements, has several times over the years launched cyber attacks against other countries, e.g. Ukraine.

One could go on showing the actual weakness of these eleven principles, but suffice it for now to point out the widespread scepticism surrounding these statements.[13] These principles are also often incorporated into norms that are now part of the criminal and civil codes of many nations, and the scepticism that can be exercised about the former spills over to the latter as a consequence. This

[9] L. Floridi, *Understanding Epistemic Relevance*, in "Erkenntnis", LXIX, 1, 2008, pp. 69-92.

[10] L. Martino, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale,* in "Politica & Società", VII, 1, pp. 61-75.

[11] C. Hamilton, M. Ohlberg, *The Invisible Hand. How the Chinese Communist Party is reshaping the world* (2020), Fazi, Rome, 2021.

[12] L. Yao-Huai, *Privacy and Data Privacy Issues in Contemporary China*, in Ethics and Information Technology, VII, 1, 2005, pp.7-15.

[13] G. Terzi di Sant'Agata, F. Voce, *Cybersecurity e nuovi equilibri europei e internazionali*, in "Notizie di Politeia", XXXIV, 132, 2018, pp. 99-107; G.R. Lucas, *Postmodern War*, "Journal of Military Ethics", IX, 4, 2010, pp. 289-298.

scepticism, however, could also be the product of a misinterpretation of the function of norms and principles. In reality, we cannot do anything without standards, norms, and principles.[14] The fact that norms are in many circumstances negligently disregarded or violated with criminal intentions by individuals or organisations, or rendered harmless by States, does not automatically mean that they are irrelevant. It may indeed be the case that a rule held to be inapplicable in certain circumstances, becomes applicable when those same circumstances have changed. If such rules had not been held to function in some sense even when it was not possible to apply them (or even when it was not advisable or convenient to apply them), then no authority could appeal to their legitimacy. Moreover, we must not fall victim to the naivety of thinking that standards actually become enforceable once the correct procedure to make them legal has been followed. We know that in order to be implemented in a legal system and to be recognised internationally, norms have to follow a long and complex path. Sources of law are sometimes informal and this means that the fungibility of a norm is by no means a process governed by automatisms, but also by all the obstacles, objections, of both an intellectual and behavioural nature that a norm aims to eliminate or merely circumvent. In short, norms have an evolutionary history, which is not without its shadows, and is often governed by mechanisms that are not, at least initially, brought into the light of political and legislative deliberation.[15]

As for the rules governing relations between States, the time of their gestation can be very long. The numerous treaties to curb the proliferation of nuclear weapons have required many years of close negotiations and sophisticated compromises. Information technology that can be used in strategic contexts (i.e. potentially all of them) certainly pose specific problems, since the technological equipment to carry out an operation to sabotage a nation's electricity system, for instance, is already available, or if it is not currently available, it may only need a new programme that a hacker could be inventing at this very moment. However, this is not necessarily an obstacle to international standards being developed to avoid disasters to ICT infrastructures that are often shared by several States.

4. The application of a norm, also implies the ability to exercise both credible deterrence and the threat of retaliation.[16] This credibility can only be made possible by an agreement between states, and particularly in our present case between the United States, the European Union, China, India and Russia. Some argue that the

[14] P.J. Verovsek, *Against International Criminal Tribunals: Reconciling the Global Justice Norm with Local Agency*, in "Critical Review of International Social and Political Philosophy", XXII, 6, 2019, pp. 703-724; C.E. Pavel, D. Lefkowitz, *Skeptical Challenges to International Law*, in "Philosophy Compass", XIII, 8, 2018, pp.1-14.

[15] C. Bicchieri, *Norms of Cooperation*, in "Ethics", C, 4, 1990, pp. 838-861.

[16] J.-P. Dupuy, *On the Rationality and Ethics of Nuclear Deterrence*, in "Philosophical Journal of Conflict and Violence", V, 1, 2021, pp. 135-138.

very nature of some cyber attacks makes the idea of deterrence something completely different from that which can be exercised by nations with armies or nuclear arsenals.[17] But even in this case, proponents of the rules argue, there is no alternative to reduce risk other than the combined use of diplomacy, deterrence, and threat. However, it is not always clear what deterrence can be used against a small group of cyber criminals, perhaps barricaded in some remote mountainous region of Afghanistan or able to make themselves untraceable in cyber space.

The very notion of cyber space implies the recognition that in this space, the information space, there are no national borders. At the same time, it is difficult to draw the boundaries between what constitutes a threat to the public and what constitutes a threat to a private individual, be it an individual or a commercial company or an industry. This could lead to a widening of the limits of State intervention in spaces that are currently recognised as the exclusive domain of the individual (assuming that such limits are always clear at the moment).[18]

Furthermore, at least in democracies, the security of industrial companies that constitute strategic assets for the State where they are established is not considered (so far) the exclusive competence of the State, but is left to the initiative of the company itself. This could be considered bizarre. After all, if the possibility of a bank robbery requires the police to intervene with preventive repressive initiatives, it is not clear why this should not be considered indispensable also in the case of theft of industrial secrets. Not all banks are equipped with security personnel, as is evident from everyone's experience. This happens because the threat and deterrence capacity of the State is considered sufficiently solid.

The reputation of the State as an enforcement agent may sometimes be sufficient to limit large investment in security when it comes to threats of aggression against individuals or theft of physical property. But in the case of assets in the so-called infosphere, things seem to be more complicated, because inadequate defence by private companies can have important effects on large areas of public interest, whereas this effect is, in principle, more limited in the case of a robbery or theft in a private home. As is said among strategy practitioners, cyber space has become the fifth territory, after land, sea, air, and extraterrestrial space where conflicts are fought. [19] Many nations have now equipped themselves not only with police departments specialised in the recognition of cybercrimes, but also with sectors of national armies that deal primarily with cyber warfare.[20]

[17] M. Taddeo, *Deterrence by Norms to Stop Interstate Cyber Attacks*, in “Minds and Machines”, XXVII, 3, 2017, pp. 387-392.

[18] L. Floridi, *Four Challenges for a Theory of Informational Privacy*, in “Ethics and Information Technology”, VIII, 3, 2006, pp.109-119.

[19] F. Rugge, *'Mind Hacking': La guerra informativa nell'era cyber*, in “Notizie di Politeia”, XXXIV, 132, 2018, pp.108-117.

[20] D.J. Lonsdale, *The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios*, in “Journal of Military Ethics”, XIX, 1, 2020, pp. 20-39.

While in the recent past it was imagined that a conflict involving a nuclear actor could be initiated by the detonation of a low-power nuclear device to disable all electronic equipment in a limited area, this now seems to be an outdated notion, superseded by the possibility of achieving the same objective through a cyber attack, which may be difficult or impossible to detect as to its origin and perpetrator.

What is often emphasised, also with regard to the possibility of introducing rules and sanctions in the case of hostile actions, is that cyber warfare actions do not have the same significance as real military actions, because they do not involve the use of troops on the ground, or missiles fired at military or civilian targets, or the use of naval forces to block a port. After all, are there absolute numbers of casualties caused by cyber attacks anywhere? Cyber warfare activities would therefore be parasitic, especially in the case of wars and hostile actions of States, compared to other activities on the ground.[21] However, the same could probably be said of activities carried out by individuals or criminal groups. These are also activities that are carried out not for the sake of doing them (unless they are carried out by some narcissistic nerd), but for profit. In addition, cyber actions for political purposes can also be carried out by terrorist groups that do not necessarily have close ties to States. What is not yet clear, however, is that cyber attacks by States could generate the typical dynamics of escalation and lead to conflict on the ground. Perhaps this is not so difficult to imagine, however. All armies are closely dependent on civilian infrastructures that are not primarily used for military purposes, with the only exception of military bases. These infrastructures can be the targets of cyber attacks. The damage that can be caused by such attacks can be very significant. Let us think of a cyber attack that manages to shut down the electrical systems of hospitals and is preparatory to a traditional military attack: such an attack could damage the logistical network of defence forces. [22]

Prior to the Russian Federation's invasion of Ukraine, numerous cyber attacks were carried out over the years. It is clear that many of these were aimed at testing Ukraine's security level, as well as creating multi-billion dollar damages. With the spread of the internet, the increasing and pervasive use of big data, networked home appliances, and the forthcoming use of exoskeletons for military and medical use, any device connected to the Internet could be the target of a cyber attack. Attacks are therefore set to increase exponentially.

The history of cybercrime and military or industrial espionage operations coincides almost perfectly with the history of the Internet. The first cyber attacks

[21] E. Barrett, *Warfare in a New Domain: The Ethics of Military Cyber-Operations*, in "Journal of Military Ethics", XII, 1, 2013, pp. 4-17.

[22] D. Whetham, *'Are We Fighting Yet?' Can Traditional Just War Concepts Cope with Contemporary Conflict and the Changing Character of War?*, in "Monist", XCIX, 1, 2016, pp. 55-69.

date back to the beginning of the 1980s.[23] It is precisely the impressive, but predictable, increase in cyber attacks that should lead us to rethink the concept of deterrence and the function of norms, argue those who are not sceptical about the implementation of principles and norms of regulation and repression.

There is an obvious difference between nuclear deterrence, encapsulated in the acronym MAD (Mutual Assured Destruction)[24] and deterrence that is exercised towards those who commit cybercrimes. In the first case, deterrence is the credible threat exercised to avoid a single event. Indeed, in the case of a nuclear attack resulting in *retaliation*, there would most likely not be a third move. In the second case, this is often comparable to the usual preventive activity of law enforcement agencies. This preventive activity does not end with the credible threat of repressive activities, but also includes educational activities among the general population to make them aware of activities that could have criminal profiles. The problem of course is that, if this is indeed one of the functions of legislation, individuals and criminal groups are certainly not impressed by it, especially when it is possible to commit crimes with the near certainty of not being caught. This is by no means to say, however, that deterrence is not important in preventing cyber attacks by States. The fact is, that this deterrence cannot be exercised through cyber tools alone. In fact, the USA has repeatedly stated that it reserves the right to respond to a cyber attack through instruments of its own choosing.[25] The response is clear and has been effective, at least judging by what has so far, to our knowledge, not happened. There have been no attacks on USA infrastructure to date that would cause visible damage on a large scale.

Deterrence is therefore constituted in the latter case by the ability to use conventional military means and the proclaimed intention to be able to treat even espionage incidents as military attacks. If the capacity for deterrence is real, then the initiative is left in asymmetric situations in the capacities of those who possess it. Also in the case of confrontation between superpowers, however, a combination of these factors may influence confrontation strategies, leading to a more careful calculation of the costs and benefits of a cyber attack.

The proposal put forward by the Russian Federation to ban all electronic warfare instruments therefore resembled more of a propaganda boast than a concrete proposal, and was intended to provoke a negative response from the United States. In the meantime, China remained silent, and the reasons for this are quite clear. These reasons are linked both to China's project of hegemony in the international arena and to the internal control systems that make massive use, at least in the cities,

[23] B. Middleton, *A History of Cyber Security Attacks. 1980 to Present*, Auerbach Publications, New York, 2017.

[24] T.W. Luke, *The Discourse of Deterrence: National Security as Communicative Interaction*, in "Journal of Social Philosophy", XXI, 1, 1991, pp. 30-44.

[25] C.L. Glaser, *Deterrence of Cyber Attacks and U.S. National Security*, The George Washington University, Cyber Security Policy and Research Institute, Report GW-CSPRI-2011-5 , 2011.

of tools for the computer control of the population, both to implement the so-called "social credit" system and to monitor the use of social networks and control the flow of news.

5. The UN did not accept the demagogic Russian proposal, but set up numerous discussion and focus groups between members of the organization. Some brought together a small number of diplomatic representations, while others were open to contributions from anyone. The result was the formulation of those principles that I mentioned at the beginning and that have been adopted by some States. There is, however, a general principle underlying these principles, namely that international law is the basis of these norms, which are adopted voluntarily and in a non-binding manner by States. The fact that they are adopted voluntarily and on a non-binding basis simply reflects a feature of the system of international law itself, which cannot be regarded as analogous to criminal, civil or administrative law adopted by a state.[26] In this case, principles, norms, rules have binding force. However, even if one must recognise the importance of having established these non-binding principles that can only be assumed on a voluntary basis, the ambiguity of some of them remains. This ambiguity is not so much in the way the principles have been enunciated nor in their substance, but rather in the nature of things. For example, the principle that civilian infrastructures should not be attacked is apparently very noble, but completely unworkable, since, as aforementioned, the military capabilities of a State depend on the massive use of civilian infrastructures. In the event of conflict, for example, roads are a military tool, and so are ports, airports and railways, all of which depend to a large extent on computer systems. Even the discussion groups that were set up as panels open to anyone wishing to make a contribution, with the help of NGOs and private companies, did not come up with any proposals that went beyond the 11 non-binding principles. They merely reiterated the relevance of international law for cyber activities. Nothing more than a tautology with respect to what has already been previously elaborated, and probably could not be otherwise. [27]

Other international discussion panels have proposed the introduction of more specific rules, such as a ban on the use of bots to enter the civilian computer systems of States. This would basically amount to a ban on launching cyber attacks, which is precisely what is being discussed. The introduction of more specific rules may however be of considerable importance because it signals the evolutionary mechanism that is also present in the case of principles, standards, rules, norms which start from general statements and become more and more specific. However,

[26] F. V. Kratochwil, *Rules, Norms, and Decisions: On the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs*, Cambridge University Press, Cambridge, 1989.

[27] S. Pietropaoli, *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in 'Rivista di filosofia del diritto', VIII, 2, 2019, pp. 379-399.

there is also a risk that must be pointed out. Since we are dealing with a field where technological innovations follow at a very rapid pace, the introduction of excessive specification could simply be pointless, because it could be outdated in practice.

Principles, standards, rules, norms are implemented at a much slower pace than in the realities we are seeking to regulate. This, moreover, is consistent with their nature as *ex post* instruments. Further concerns arise from the possibility of unintended consequences of using cyber attacks. These could be launched with the idea of testing the reaction capabilities of the antagonist, but could have unintended consequences of a far greater magnitude, thus provoking an escalation.[28] Precisely for this reason, some think that treaties similar to the nuclear weapons treaties could be signed, for instance to limit the use of certain cyber resources. However, it is not clear what these resources should be. Should the use of supercomputers be restricted by limiting their computing power? This seems an entirely unrealistic hypothesis for several reasons. First of all, it is likely that more and more computing power will be needed to integrate civil infrastructures with each other. Secondly, this same power may be needed to develop increasingly sophisticated cyber defence tools to guard against increasingly sophisticated threats.

Many ICT resources are in the hands of private companies in that part of the world where representative democracies and market economies prevail. It is not certain that this situation will continue in the future. Some ICT resources are already considered strategic for the security of States, and all States have sufficiently flexible rules to be able to quickly include some sectors within those that must be supervised because they are crucial for national security. Leaving aside for the moment the case of states where this supervision is well established, such as China, where all companies of a certain weight are considered potentially strategic and are participated in by bodies that can be traced back to the Chinese Communist Party, democratic governments may also want to control private companies that have actual and/or potential interests in the field of security. Even now, in some states, private companies are not allowed to actively respond to malicious attacks with reprisals.

The so-called "reputation effect" can play a role in the development of security standards. Being considered a 'rogue state' has not only reputational but also economic effects and could undermine the internal stability of certain States. There are instruments of war that are banned by international treaties, such as chemical and biological weapons. This does not at all mean, as is easily imaginable, that some States are not developing them or do not possess significant stockpiles of them.

This, however, cannot be done publicly, because it would provoke sanctions and other hostile acts by other States that would feel threatened by them. Something similar could perhaps be imagined in the case of States using private companies to

[28] L. Carlson, R. Dacey, *Social Norms and the Traditional Deterrence Game*, in “Synthese”, LXXIV, 1, 2010, pp. 105-123.

carry out 'proxy cyberwars'. [29] The damage to a State's international reputation is sometimes also measured by the real or advertised possibility of causing a high number of victims among the civilian population with weapons banned by international conventions, such as chemical, biological or nuclear weapons, or conventional weapons such as phosphorous bombs, cluster bombs or special anti-human mines.

In the case of these weapons, one can well and easily imagine high representatives of a State appearing in international forum with photos of missile installations deemed to be an imminent threat to their security, as happened in the 1962 Cuba crisis, or showing alleged evidence of the manufacture of weapons of mass destruction, as happened before the USA invasion of Iraq. It is hard to imagine something similar in the case of a cyber attack. It is unrealistic to believe that high-ranking figures would gain media attention, usually needed before a military intervention, by publicly exposing parts of a code. Moreover, intrusions into computer systems with high protection thresholds often arouse admiration, because writing malicious code is considered an esoteric skill reserved for a few. In addition, these intrusions usually do not immediately provoke military and/or civilian victims, as is the case with a military attack.

One might think, however, that the principle prohibiting attacks on civilian infrastructures such as hospitals also applies to its computer facilities. In this case, perhaps, the reputational effect could be similar to that affecting *rogue States* that use weapons banned by international conventions. On the other hand, the very high interconnectedness of computer network structures could make it difficult to understand whether the main target of an attack is, say, a health infrastructure, or whether the damage caused to it is an unforeseen and unintentional side-effect.

6. It is not at all clear how a treaty for limited use of cyber tools in case of attack or defence would work.[30] To date, attacks have, to the best of our knowledge, also in the case of armed conflicts, concerned infrastructure linked to military or financial objectives. In the case of attacks on civil infrastructures, such as the recent attack against the Italian State Railways, the malicious intention seems to be to obtain a ransom to unlock the site that has been hacked.

Whether a hostile state is behind this attack (the name that has been mentioned is of course the Russian Federation) is not certain. It could be that this or other attacks have been piloted by States and that the intelligence agencies of the affected countries know about it with reasonable certainty, but do not want to propagate it so as not to trigger an escalation. As mentioned above, there is apparently a broad

[29]J. Collier, *Proxy Actors in the Cyber Domain: Implications for State Strategy*, in “St. Antony's International Review”, XIII, 1, 2017, pp. 25-47.

[30]J. Goldsmith, *Cybersecurity treaties. A Skeptical View,*
https://www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf.

consensus on the need to regulate cyber space precisely to avoid possible escalation, but where precisely one should draw the boundaries that could lead to it is a matter of dispute.

Those who are sceptical about the scope and effectivity of international law draw one of their recent arguments precisely from the anarchy of cyber space.[31] For example, as early as 2015, the USA and China agreed on the need not to use cyber espionage tools to gain commercial advantage. However, this agreement has been largely disregarded, precisely because of other political and economic circumstances. Moreover, it is doubtful that a State that is the antagonistic power of the USA can and will distinguish between political and economic conditions. Principles, norms, and rules must first and foremost come to terms with its hegemonic design. What exactly is an act of commercial espionage as distinct from an act of military espionage? What is an act of political espionage as distinct from an act of commercial? It is clear that, for instance, an act of political espionage could result in a commercial advantage. These activities intersect with each other and it is often simply not possible to distinguish between them.

International treaties represent a grey area masked by the assertiveness of principles. On the other hand, it is perhaps precisely this grey area that many times advises against violating them. What I mean, is that to violate or not to violate a treaty, an agreement, a declaration of intent, provided it is clear what has happened and who has committed it, is a matter of calculating expected utility and not of adhering to principles.

The problem is not one of adhering to principles, but of making it inconvenient to violate them too freely.[32] However, the problem that always remains is that of providing the punishment for the offender. This cannot be done by means of a supranational state, which neither exists at the moment nor is on the distant horizon, but only through the instruments that the planetary superpowers already have at their disposal. This sounds like a trivial truism, but it makes it clear that principles, norms and rules follow the flow of political power and the calculation of utility. This is clearly due to the integration of these hostile activities both in the constant competition between states and in the potential activities on the battlefield.

In fact, the US Cyber Command adopts the strategy of 'persistent engagement', which is the same strategy that has been consistently used since the end of World War II.[33] *Persistent engagement* has many advantages, but mainly two: the constant pressure on the infrastructures of potentially hostile states, as demonstrated also by

[31] L. Lessig, *The Zones of Cyberspace*, in “Stanford Law Review”, XLVIII, 5, 1996, pp. 1403-1411.

[32] J. Goldsmith, *Against Cyberanarchy*, in “The University of Chicago Law Review”, LXV, 4, 1998, pp. 1199-1250.

[33] M.P. Fischerkeller, R.J. Harknett, *Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation*, 'The Cyber Defence Review', IV, 2019, pp. 267-287.

Israel's sabotage of the Iranian nuclear programme; the flexibility in the choice of response that is not bound to a precise system of rules.

International armaments treaties can also contain lists specifying which behaviour should be considered as accidents. This is already the case in other fields, e.g. when warships are involved. The same questions that have been raised on other occasions in these pages probably arise again here, since while it is easier to ascertain in non-virtual reality that can be defined as an accident, this can be difficult in cyber space. If a warship or a fighter plane has a malfunction, perhaps involving traditional radio communication systems, they might still be able to signal their non-hostile intentions in some other way when trespassing in potentially hostile territory.

In the case of cyber space however, it is not at all clear how this could happen. Perhaps by communicating one's intentions in a timely manner and providing potentially malicious code? On the other hand, a code that is potentially harmful to the adversary constitutes a clear competitive advantage, so it is not clear why it should be shared unless there is a credible threat of retaliation.

There is a further difficulty regarding international treaties to limit the use of cyber attack tools, which can be deduced from the history of the numerous US-USSR negotiations to limit nuclear weapons. In that case, there were control instruments to verify the application of the treaties. For instance, commissions that met periodically to verify progress in the application of the treaties, periodic inspections of sites of interest, the possibility of reconnaissance flights over sites of interest, and so on. In the case of prevention of cyber attacks, it is difficult for the moment to even imagine what these instruments of control and prevention might be.

In the case of incidents, control and verification could obviously only be *ex post* and could certainly have a decisive usefulness to prevent future incidents. But in the case of verifying the good intentions of the parties to a treaty, what should be done? Inspect the sites where government servers reside and the programmes installed there? But this could easily turn into an espionage operation. Launch bots with surveillance functions, then? Here too, the same difficulties could arise.

7. It could be said that these objections relate to technical difficulties and are therefore not insurmountable in principle. This is a serious line of argument and is in fact presupposed by all proposals that have been made in this field to prevent cyber attacks and cyber incidents. Also, in the pre-war meetings between the Russian Federation and the US, proposals were made to precisely delimit the infrastructures that should under no circumstances be subject to cyber hostilities.

Among them, President Biden proposed communication infrastructure, energy, financial services, and ICT itself, (at least according to press reports). However, this list seems to be more of a propaganda operation than a concrete operational proposal. On the other hand, important agreements have often started with this kind of communication. Biden added that the US has the necessary tools to retaliate in the event of attacks on these facilities. One could also speculate that the areas that have not been named are therefore possible targets for cyber attacks that would not involve retaliation but frankly, I think that the usual logic is of little help in drawing reasonable conclusions in this area.

Cyber wars sometimes look like proxy wars fought by cyber mercenaries. It is easy to imagine that behind these cyber mercenaries there are often governments, since it is obvious that even just to intervene in espionage activities on the undersea backbones carrying fibre optic cables requires investments that only a State can afford. However, there are reasons not to be completely pessimistic about the formulation of principles, rules and norms at international level.

Foremost, their formulation and signing signals that there is an agreement involving several parties. This is not realistically sufficient. For example, the International Criminal Court has also been joined by many states, but it is not joined by the USA, China or Russia, among others. Certainly this is not a necessary reason not to continue its work. Appealing to signed treaties justifies and makes credible acts of limited retaliation. As usual, the ability to access a threat must be credible, but publicly implementing rules seems to be a necessary preliminary step to retaliation, at least if the State is not a *rogue state*. One could imagine that retaliation is not only an act of force, but could consist of credible deterrent acts. One could imagine that some more stringent rules would work for allied countries (EU and NATO) and others less stringent for other countries and that the former would be associated with benefits for the contracting parties. The more strategically important States subscribe to such rules, the more they will be inclined to impose sanctions or limit cooperation on other states that do not subscribe to them. This is happening in many areas of relations between States, and certainly not since today. Whether this is enough to render inadequate Hobbes' notation that relations between States reproduce the state of nature is *wishful thinking* at present.