Artificial Intelligence for Human-Technologies-Economy Sustainable Development
23–25 May 2024
Lublin, Poland
make learn
TIIM
PIConf
Management, Knowledge and Learning
International Conference
Technology, Innovation and Industrial Management
Sustainable Development

Ukraine: A Great "Training" For International Law

Ciro Settecasi
Società Italiana di Storia Militare (SISM)
ciro.settecasi@gmail.com

Abstract

The aim of this paper is to highlight the inadequacy of International Law with respect to hybrid warfare and the consequences that are affecting the Ukraine-Russia front. The war in Ukraine is not only a hybrid war but is also extended to all the characteristics of cyberspace and new social media, presenting many novelties that have to do with the digital context. A war that poses new stakeholders and instruments, such as hackers, influencers, misinformation, cryptocurrencies and wallets. In the conflict in Ukraine, tech platforms, groups of hackers operating globally and affecting both sides in the conflict, are acting. Rapid technological advancement has led to a strong distrust of international regulation, i.e. the full application of International Law in the field of cyber security: hackers, cyber-warfare events and cyber-attacks. All that has been highlighting all the limits of International Law, which still fails to protect a State that could suffer threats and/or attacks and that could lead to any diplomatic escalation against a possible threat. The use of cyber means to damage and/or annihilate enemy infrastructures is, to all intents and purposes, a "declaration" of cyber-warfare, which also generates important consequences for the living standards of the civilian population. Another critical aspect is the fact that the actors responsible for the attacks are not always identified: most of the time, it is difficult to attribute responsibility to the subject, making it impossible even to apply a form of "punishment". The International Community is required to implement legislation that exclusively regulates the cases affected by digitalization. "One small step for a man, one giant leap for mankind" is common sense if we think of the security of the population itself; in particular, implementing a new branch of International Law fully dedicated to cyber-warfare is a necessity of primary importance in a geopolitical context that is constantly evolving from an IT and digital point of view.

Keywords: hybrid warfare; misinformation; cyber security; misinformation; cryptovalute

INTRODUCTION

The conflict that Europe has been witnessing for some years has put a strain on the international order in the context of the battle in the information domain (big tech technology platforms, crypto, new social media, hacking). International law, in fact, must regulate both the "Internet" and the human behaviors that take place on it and adopt a series of adjustments for the management of information on the network. Over the years, technological progress has changed state legal systems, including international ones, such as the numerous rules negotiated to regulate the behaviour of states in outer space, civil aviation and the use of drones, the use of geostationary orbit and nuclear energy. Unlike purely technical changes, in the case of the Internet, information dynamics have impacted and are still changing all international legislation, starting from the "model" of regulation of the domain name system, the so-called domain name system (DNS)[1] of the Internet. Often, such a process is not easy to identify, especially in the context of hybrid warfare - "Gerasimov's"[3] doctrinal concept.

In the very nature of the International Community, States form a society which, like every human society, requires, postulates and sets rules aimed at regulating social relations, ordering coexistence and cooperation among the members of the society in question. Given that the I.C. lacks superordinate structures with an empire over sovereign states, it is essential through international law to provide the I.C. with rules aimed at ordering its relations. It is obvious that, in the absence of structures superordinate to the states, all the essential functions of the system in question are centred on the states themselves. It is the States, in fact, that create international norms in different ways and through different processes that will be discussed shortly: in other words, it can be said that States are both the legislators and the main recipients of this law. In the same way, ex nihilo, States also regulate the International organisations to which international rules are addressed. The absence in the

[1] The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the management and coordination of the Internet domain name and address space, which are critical resources necessary for Internet connectivity. Though international in reach since it cooperates with persons, organizations and governments in many countries, ICANN was set up as a private non-profit organization under California law. This article examines the role, legal nature and basis of ICANN and the domain name system (DNS). It first maps and analyses the various regulatory instruments underlying ICANN and the DNS. What emerges is that, very often, several and different modes of regulation, both formal and informal, are required to address a particular issue satisfactorily. The article examines whether and to what extent these different types of instruments co-exist and interrelate as one coherent regulatory framework. To do so, this article draws upon Teubner's notion of hybrid networks and makes an analogy with modern theories on how various sources of law apply within a legal system. In particular, it follows and builds upon Ost and van de Kerchove's notion ofnetwork or 'mesh' regulation. Cafaggi's notion of contractual networks is utilized to explain the contractual web at the heart of the gTLD namespace.

[2] Hybrid warfare is a phrase that illustrates today's war in terms of making, conceiving, and thinking about war. Tanks, trenches, soldiers, and bayonets are a thing of the past. Terrorism, psycho-cognitive manipulation, disinformation, speculative finance and hackers are the present and the future. The strength of hybrid warfare is precisely the unpredictability that is difficult to neutralize.

[3] Valery Vasilyevich Gerasimov is a highly decorated general from Kazan, the "third capital of Russia", and has been the Chief of Staff of the Armed Forces of the Federation since 2012. Gerasimov, born in 1955, has dedicated his life to the army: he entered the Suvorov Military School as a young man, from which he graduated in 1973, and has worn the uniform since he was little more than a teenager.

[4] International organizations are precisely the most sophisticated of the instruments of international cooperation that have ever been invented: by means of agreements between them, two or more States create appropriate organic structures – that is, institutional apparatuses – to which they entrust the task of pursuing the common interest through joint action in a given sector, attributing to each of these organizations the competences and means deemed necessary. If this or that organization is empowered to conclude agreements with congener entities or with States, it is because the founding treaty has explicitly or implicitly provided for it. In short, although it can be recognized that organizations are to be considered

an international community of a centralized organization of the type that exists in state systems might seem to be a limitation, but the organization of state systems and that of the international order remaincompatible and can coexist, i.e. the I.C. it is a society of equals, of coordination and not of subordination; The international community, therefore, has no authority superior to the States, that is,the power to compel the States to respect the rules they have set for themselves.

As is the case with other legal systems, international law reveals its fundamental characteristics through the principles relating to the subjects, the ways of creating rules, the means of resolving disputes, and the ways of ensuring compliance with the rules. Unlike domestic law, in which the power from which legal norms emanate is also expressed in the sense of imposing and guaranteeing legal subjectivity on the entities to which it is addressed, in International Law, The absence of a centreof power superior to the basic subjects that is endowed with the ability to impose subjectivity preventsus from conceiving that a normative gap can be produced between international relations and the lawthat governs them. This is the so-called "principle of effectiveness", the foundation of the system.

Obviously, all international organizations are and remain "creatures" of States, that is, entities desired by them, built and regulated as instruments of cooperation between them: the founding act of each of these is always an international agreement, the result of the sovereign will of the States that give life to it by endowing it with organs, determining its functions, competences and powers.

At the "universal" level, the United Nations (UN), with its vast organic apparatus, and UNESCO, the International Labour Organization (ILO), the Food and Agriculture Organization (FAO), the World Health Organization (WHO), the International Monetary Fund (IMF), the International Bank for Reconstruction and Development (BIRD) and the World Trade Organization (WTO); All of them form a permanent framework of planetary cooperation.

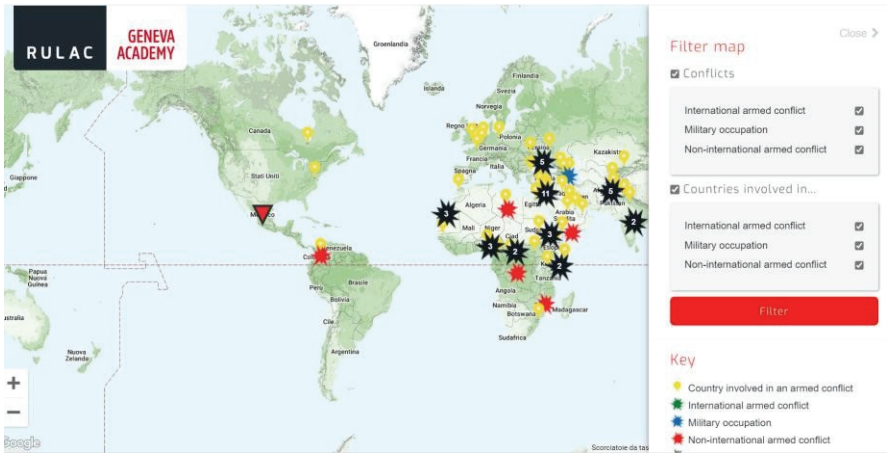
At the regional (or sub-regional) level, states are increasingly grouping together in very numerous organizations, pursuing common interests such as the European Union. Despite being a pillar of contemporary society, the European Union has been witnessing, for some years now, a strong crumbling of the international order in the context of the battle of the information domain. International law, in fact, must regulate both the "Net" and the human behaviors that take place on it, and adopt a series of adjustments for the management of information on the Net. Over the years, technological progress has changed state legal systems, including international ones, such as the numerous rules negotiated to regulate the behaviour of states in outer space, civil aviation and the use of drones, the use of geostationary orbit and nuclear energy. Unlike purely technical changes, in the case of the Internet, information dynamics have impacted and are still changing all international legislation, starting from the "model" of regulation of the domain name system, the so-called domain name system (DNS[5]) of the Internet. Often such a process is not easy to identify, especially in the context of hybrid warfare, the doctrinal concept of "Gerasimov[6]".

subjects of international law, it must also be emphasized that they are not hierarchically placed above States, since it is precisely States that created them and support them as instruments of cooperation among themselves

INTERNATIONAL INVOLVEMENT

In these days, and for too long now, in cities other than Ukrainian ones such as Mariupol, Odesa, Kharvik, Beit Hanun, and Gaza, as well as in hundreds of other conflicts around the world[7], the tens of millions of dead echo Nazi-fascism and the atomic bomb and do not seem sufficient for the banning of wars and for the full affirmation of the principles expressed by the United Nations, understood as the democratic institution entitled to represent the interests of the planet and of the whole of humanity,respected and recognized by all nations. And, from these, they are fully entitled to settle conflicts between states, by the way of law and negotiation, without resorting to wars, unilateralism and even less to thearms race, as has been happening in recent times. The more science grows, the more technology develops, the more there is a need for peace. Pace che la stessa Europa non è in grado di riconquistaresoprattutto vicino i propri confini.

It is clear that there is an urgent need to change the current model of development, as the most enlightened scientists strongly argue.



[5] The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the management and coordination of the internet domain name and address space, which are critical resources necessary for internet connectivity. Though international in reach since it cooperates with persons, organizations and governments in many countries, ICANN was set up as a private non-profit organization under California law. This article examines the role, legal nature and basis of ICANN and the domain name system (DNS). It first maps and analyses the various regulatory instruments underlying ICANN and the DNS. What emerges is that, very often several and different modes of regulation, both formal and informal, are required to address a particular issue satisfactorily. The article examines whether and to what extent these different types of instruments co-exist and interrelate as one coherent regulatory framework. To do so, this article draws upon Teubner's notion of hybrid networks and makes an analogy with modern theories on how various sources of law apply within a legal system. In particular, it follows and builds upon Ost and van de Kerchove's notion of network or 'mesh' regulation. To explain the contractual web at the heart of the gTLD namespace, Cafaggi's notion of contractual networks is utilized.

[6] Valery Vasilyevich Gerasimov is a highly decorated general from Kazan, the "third capital of Russia", and has been the Chief of Staff of the Armed Forces of the Federation since 2012. Gerasimov, born in 1955, has dedicated his life to the army: he entered the Suvorov Military School as a young man, from which he graduated in 1973, and has worn the uniform since he was little more than a teenager.

[7] The War Report 2014: 29 of the armed conflicts were 'non-international' in character, between non-state armed groups or between one or more States and one or more non-state armed groups. These conflicts took place in 18 States: Afghanistan, Central African Republic (CAR), Colombia, the Democratic Republic of the Congo (DRC), Egypt, India, Iraq, Libya, Mali, Nigeria, Pakistan, Somalia, South Sudan, Sudan, Syria, Thailand, Ukraine and Yemen.

In this global scenario in which the “tertium non datur” reigns, the I.C. recognizes international organizations to pursue and implement International Law considering a current scenario in which the transnational power of platforms and cryptocurrencies is increasingly ambivalent[8].

THE WAR AT THE GATES

Under the eyes of world public opinion, the war in Ukraine is not just a hybrid war; it is extended into cyberspace and documented ad horas on social media, presenting many innovations that have to do with the digital context. A war that recalls the dawn of the twentieth century for the triggering reasons (aggression against a sovereign state) but also conducted with the tools of the twenty-first century because it sees the irruption of new actors and/or tools, of hacking, of platforms, of social media, cryptocurrencies and wallets.

In the conflict in Ukraine, tech platforms, hacker groups operating from all over the globe but affecting the infrastructure of countries in conflict, influencers[9], endorsements, cryptocurrencies between funding of various kinds and social networks between disinformation[10] and effective[11] communication have acted. Last but not least, donation crowding has made its debut in recent years to support Ukrainian citizens by raising more than 25 million euros[12].

[8] Altalex "Cyber war and the law of war: the answers that international law does not have" by Claudia Morelli".

[9] The prime ministers of Poland, Lithuania, Latvia and Estonia have made an appeal, writing directly to the CEOs of Google, Facebook, YouTube and Twitter, to ask them to do more to counter disinformation linked to Russia's invasion of Ukraine. "They urged companies to suspend the official accounts of Russian and Belarusian government institutions, state-controlled media, and personal accounts of the countries' leadership that constantly spreading disinformation about the situation in Ukraine."

[10] Meta, the company that owns Facebook and Instagram, has blocked 40 accounts deemed to be a Russian disinformation network (Source: Ansa), identifying more than 1 billion pieces of spam content. The news was given with a post on the company's official account and here you can read the news on the official website.

[11] Youtube has blocked channels linked to RT and Sputnik in the EU, and announced this with a post on Twitter, while a spokesperson for the platform created by Jack Dorsey said it had suspended a dozen accounts that violated the rules against the manipulation of the platform (Source: Open on line). Google Maps has disabled Google Maps features, which provide live data on traffic conditions in Ukraine, to prevent them from being used by Russian troops to track the movements of the Ukrainian military. This was confirmed by the company to Vice, after a series of reports from people who were using the service to track the movements of troops and civilians during Russia's invasion of Ukraine (Wired). Google's announcement came a day after Ukrainian authorities ordered to dismantle or erase road signs across the country to slow Russia's advance. The order was given on a Facebook post by the Ukrainian road authority, accompanied by the comment "the enemy has a pathetic internet connection and does not know how to orient himself in the area. Let's help them go straight to hell," the newspaper said.

[12] "Money: Crypto Platforms Don't Freeze Russian Funds: Is Alibi for a Crackdown Coming?

Big tech platforms, in short, are actively participating in the field of war operations but at the same time, they mark a further limit in the field of European Union International Law without ensuring, among the various sanctioning tools, to weaken the largest Russian investors who circumvent the various embargoes and/or UN/European solutions by investing in cryptocurrencies and/or crypto-exchanges. Not even the Ukrainian minister's appeal to the Binance agency to freeze all accounts belonging to Russian citizens has had any effect, so much so that both the Binance agency itself and Kraken have stated that they will not unilaterally freeze the funds of thousands of Russian citizens through no fault of their own, also recalling that cryptocurrencies are intended as a means of ensuring great independence and financial freedom around the globe. According to calculations by Saxo Bank, the value of cryptocurrencies in the hands of Russian citizens today is about $200 billion. According to the chart, real flows from ruble to Bitcoin hit their highest level in about nine months, inversely charting the Russian currency's steep course after Western sanctions.

Many stakeholders have intervened in support of the Ukrainian cause: from the CEO of Apple who has stopped the sale of hardware in Russia to the company Snapchat that has blocked Russian advertisers, not least the hackers who have operated against the Russian offensive in multiple IT

sectors, including the military. E.g. Anonymous has blocked newspaper and news sites, the website of the Duma and the Russian government, news agencies, convoys (announcements follow one another on Twitter), with DDoS attacks, attacks[13] that saturate the resources of a system by essentially blocking it, but not destroying it.

THE RESPONSE OF THE INTERNATIONAL COMMUNITY

Rapid technological advancement has led to a strong distrust of international regulation or the full application of International Law in the field of cyber security: hackers, cyber-warfare events and cyber attacks. All this has led to major repercussions on the global system, highlighting all the limits of International Law, which still fails to protect a State that could suffer threats and/or attacks and that could lead to any diplomatic escalation against a possible threat[14].

The use of cyber means to damage and/or annihilate enemy infrastructures is to all intents and purposes a "declaration" of cyber-warfare, which also generates important consequences for the living standards of the civilian population. See "Anti-aircraft defense systems have stopped working in the Kyiv region, and the internet is out of action due to a cyberattack, which may be the most powerful since the beginning of the war. A few days ago, it was Ukraine that hit: with malware that infected the Russian tax system"; Another critical aspect is the fact that the actors responsible for the attacks are not always identified: most of the time, it is difficult to attribute responsibility to the subject, making it impossible even to apply a form of "punishment".

The International Community is required to implement legislation that exclusively regulates the cases affected by digitalization. A step forward is right and necessary, common sense if we think of the security of the population itself; in particular, implement a new branch of International Law, fully dedicated to Cyber-Warfare, It is a necessity of primary importance in a constantly evolving geopolitical context from an IT and digital point of view. Currently, the IC does not have the possibility, in the event of an attack on national infrastructures of countries not at war, it can be understood as an "armed attack" (even if cybernetic). As such, governed by Article 5 of the NATO Treaty, which legitimizes the use of the right of defence under Article 51 of the Charter of the United Nations[15]:

"**Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.**"

The first question that is difficult to answer is when a possible cyberattack against a third country belonging to the Atlantic Alliance can be qualified as a military attack, such as to trigger Article 5 of the NATO treaty and therefore legitimize the right of defense, based on Article 51 of the United Nations Charter.

[13] (see Reuters: Ukraine calls on hacker underground to defend against Russia): the Ukrainian government itself has appealed to volunteer hackers from all over the world to stop the cyber offensive, "recruiting", according to some sources, over 130 thousand experts, some engaged on the cyber front (i.e. incursion into "enemy" computer systems), others on the front of the fight against disinformation.

[14] Euronews: "Cyber warfare: a hacker attack hits Ukraine's largest telecommunications provider."

[15] ART. 51 – CHARTER OF THE UNITED NATIONS.

International law defines an armed attack as a destructive, so-called kinetic attack. In doctrine, there is no common view regarding the assimilation of a cyber attack to an armed attack. Think of DDoS[16] attacks, which shut down systems but don't destroy them. The fact remains that if the cyber attack is launched against a critical infrastructure and destroys it, and therefore produces kinetic effects, it is considered armed. To give an example, Israel was the first country, in 2019, to respond with a (kinetic) missile attack to a cyber attack, as reported in the Digital Agenda (Missiles in response to a cyber attack: how Israel rewrites cyber war). Israel[17], in early May, with the aim of harming Israeli citizens, reported to the Times of Israel and to the communiqués entrusted by the Israel Defense Forces (IDF) to Twitter that the cyber attack was stopped by a team of an elite unit (about 8200 military intelligence hackers). Once the attempted attack was identified, it was contained but kept "active" for the time necessary to identify its origin and initiate a kinetic reaction against Hamas, launching a rocket counterattack aimed at "physically" destroying the origin of the attack, i.e. Hamas' cyber headquarters.

The issues that this scenario raises, from the point of view of International Law, are those of "proportionality" and the exact imputation of the cyber act to the State at war. The second aspect of cyber resistance concerns hacker actors: until now, the law of war was based on the distinction between military and civilian, between military and civilian targets. To what extent do states have a responsibility to their citizens to prevent them from provoking hostile activities?

The need to identify who the threat is and trace it back to a state is virtually impossible. Moreover, Operational Theater is completely different from traditional theaters because it is extraterritorial. Expert Farnelli: "This war is an absolute first. The law of war does not have all the answers for cyber warfare":

Ci troviamo di fronte ad un conflitto armato causato da una violazione del divieto di uso della forza, da parte della Russa, che viola il diritto internazionale e che legittima il diritto di difesa dell'Ucraina". "Sull'applicabilità del diritto bellico al cyber spazio, il dibattito in seno alle Nazioni Unite dimostra la spaccatura tra gli Stati. Negli anni si sono succeduti due gruppi di lavoro e già si sono verificate alcune fratture insanabili, proprio tra il blocco degli Stati capeggiati dagli USA e il blocco capeggiato dal tandem Federazione Russa-Cina". "Sull'applicabilità del diritto bellico al cyber spazio, il dibattito in seno alle Nazioni Unite dimostra la spaccatura tra gli Stati. Negli anni si sono succeduti due gruppi di lavoro e già si sono verificate alcune fratture insanabili, proprio tra il blocco degli Stati capeggiati dagli USA e il blocco capeggiato dal tandem Federazione Russa-Cina.

It is well established that any cyber attack on critical infrastructures and non-military targets, but also museums, places of worship or UNESCO-protected assets, can be traced back to war crimes and crimes against humanity. In this regard, the International Criminal Court (not recognized by either Russia or the US) has opened an investigation into possible war crimes and crimes against humanity committed by Russia in the invasion of Ukraine. ù The initiative could bring Vladimir Putin into the dock, as has happened to other political leaders in the past. There tends to be agreement on the applicability of the law of war to cyberspace. But there are many issues to be resolved: the equivalence between a cyber attack and kinetic attack; the difference between the levels of cyberattack that can qualify as military; and, again, the limits of kinetic attacks and proportionality, relative and reciprocal.

[16] Distributed denial of service (DDoS) attacks are one of the leading cyber threats. Here's everything you need to know. The acronym stands for Distributed Denial of Service, and consists of bombarding a site with requests, until it knocks it out and makes it unreachable. According to the latest data from Clusit, the Italian association for computer security, it is among the attacks that affect a company every five minutes along with malware and ransomware.

[17] Network digital 360 "Missiles in response to a cyber attack: how Israel rewrites cyber war".

REFERENCES

Valery Vasilyevich Gerasimov
Valery Vasilyevich Gerasimov
The War Report 2014
Altalex "Cyberwar and the law of war: the answers that international law does not have" by Claudia Morelli".
"Money: Crypto Platforms Don't Freeze Russian Funds: Is Alibi for a Crackdown Coming?
Euronews: "Cyber warfare: a hacker attack hits Ukraine's largest telecommunications provider."
ART. 51 – CHARTER OF THE UNITED NATIONS.
Network Digital 360 "Missiles in response to a cyber attack: How Israel rewrites cyber war".
Expert Farnelli: “This war is an absolute first. The law of war does not have all the answers for cyber warfare”
The Ukraine crisis timeline –
htttp://ukraine.csis.orgRulac geneva academy –
http://www.rulac.org
Carte geopolitiche limes – http://www.limesonline.com/tag
ISPI – Istituto per gli studi di Politica internazionale – https://ww.ispionline.it
IAI – Istituto di Affari Internazionale – https://www.iai.it