An Overview of International Humanitarian Law in France's New Cyber Document

by Przemysław Roguski

September 27, 2019

On September 9, 2019 the French ministry of defense published the declaration on "Droit International Appliqué aux Opérations dans le Cyberespace" (International Law Applicable to Operations in Cyberspace), a document setting out its views on how international law applies in cyberspace. The first part of the document, regarding peacetime international law, has already been analyzed at *Just Security* by Prof. Michael Schmitt and myself at *OpinioJuris.* Therefore, in this post, I will focus on the document's treatment of international humanitarian law.

General Applicability of International Humanitarian Law

The declaration on international law follows three major documents which have been published by France in the course of 2018 and 2019: the Strategic Review of Cyberdefense (Revue stratégique de cyberdéfense), the Ministerial Policy on Defensive Computer Warfare (Politique ministérielle de lutte informatique defensive) and the Public Elements of Military Doctrine on Offensive Computer Warfare (Éléments publics de doctrine militaire de lutte informatique offensive). In these documents, France develops an organisational model for its cyber armed forces as well as a military and political doctrine on cyberdefense, centered around the goals of guaranteeing the security of French information systems and achieving French and European strategic autonomy in cyberspace. This strategic autonomy includes the capability to act in all domains – including cyberspace – in the case of an armed conflict.

During an armed conflict French armed forces may resort to offensive computer warfare (Lutte informatique offensive or LIO), i.e. actions taken in cyberspace, either autonomously or in combination with conventional military means, to produce effects against an adversary computer system in order to alter the availability or confidentiality of data (but, interestingly enough, not its integrity). In doing that, France sees itself strictly bound by the rules of international humanitarian law (IHL),

which it confirms to be applicable to cyber operations conducted during armed conflicts, both international and non-international, on the same basis as they would apply to exclusively physical action:

> En situation de conflit armé, le cyberespace est un espace de confrontation à part entière qui s'articule avec les autres champs de confrontation. La capacité informatique offensive mise en oeuvre sur les théâtres d'engagement des forces armées françaises est maîtrisée à travers une doctrine et un cadre d'emploi qui la soumettent au respect du Droit International Humanitaire (DIH).
>
> In situations of armed conflict, cyberspace is a space of confrontation in its own right which is linked to other domains of confrontation. The offensive cyber capacity employed in the theatres of engagement of the French armed forces is controlled by a doctrine and a framework of engagement which require it to respect International Humanitarian Law (IHL).

Cyber operations constituting hostilities between two or more States may give rise to the existence of an international armed conflict (IAC). France is of the view that, in general, cyber operations will accompany conventional military operations, in which case the determination of the existence of an armed conflict should pose no difficulties. At the same time France does not exclude in principle the theoretical possibility of an armed conflict conducted exclusively by cyber means. It stresses, however, that in order to make this determination, these autonomous cyber operations would need to reach the necessary threshold of violence. With regard to non-international armed conflicts (NIAC), France holds that the current state of technological development seems to exclude at the moment the possibility of NIACs fought exclusively by cyber means.

France stresses that, although dematerialized, cyber operations remain subject to the geographical scope of IHL to the extent that their effects must be confined to the territory of the States Parties to the international armed conflict and/or the territory on which the hostilities in a non-international armed conflict (NIAC) take place. At the same time, NIACS may be "exported" when the parties to an initial NIAC continue their fighting in the territory of one or more neighbouring States with the consent of the State or States concerned. In this case, cyber operations conducted in connection with the "exported" NIAC must comply with the rules applicable to the original

conflict, i.e. Common Article 3 of the Geneva Conventions in case of lower-intensity NIACs and Common Article 3 and Additional Protocol II to the Geneva Conventions (AP II) in case of high-intensity NIACs.

In case of an armed conflict, the use of cyber weapons, defined as "digital means, including weapons, means and methods of digital warfare, implemented in a cyber operation against the opposing party in a context of armed conflict," has to strictly conform to IHL rules on distinction, proportionality and necessity. France stresses that the specificity and complexity of cyber operations require a risk control system just as important as that applied to conventional operations and taking into account the inherent characteristics of conducting operations in cyberspace. In practice, the risks associated with the use of a cyber weapon, particularly the immediacy of the action, the dual nature of the targets, and the interconnectedness of networks, require a specific digital targeting process encompassing all phases of the cyber operation, in order to subject them to the principles of distinction, precaution and proportionality, particularly with a view to minimizing potential damage and civilian casualties.

Cyber Operations as Attacks within the Meaning of Art. 49 of AP I

> [Cyber-]opérations peuvent constituer des attaques au sens de l'article 49 du Protocole additionnel I aux Conventions de Genève (PA I), dès lors qu'elles produisent des dommages physiques, ou qu'elles rendent un système inoperant.
>
> Cyber operations may constitute attacks within the meaning of Article 49 of Additional Protocol I to the Geneva Conventions (AP I), if they produce physical damage, or if they render a system inoperative.

In France's view, every cyber operation undertaken in the context of an armed conflict and constituting an act of violence against the adversary, whether in offence or in defence, qualifies as an attack under Art. 49 Additional Protocol I to the Geneva Conventions (AP I). In discussing the necessary threshold of violence, France takes issue with Rule 92 of the *Tallinn Manual 2.0,* which states that the notion of "attack" requires certain material effects in the form of injury or death to persons or damage or destruction to objects. Based on the fact that the primary target of a cyber operation is not a person or object, but a computer system or other electronic equipment, France is of the opinion that a cyber operation already constitutes an attack when the adversary's equipment or systems no longer render the service for which they were set up, whether temporarily or permanently, reversibly or not. This is demonstrated by

way of the following example: the destruction of an adversary's offensive or conventional military computing capabilities either by disruption or infliction of major (physical) damages is an attack within the meaning of IHL.

Similarly, an attack should also be assumed if the same effect is produced by destroying computer equipment or systems, or by altering or deleting digital data and/or data flows which render inactive a service essential to the functioning of these capacities. In the case of temporary and/or reversible effects, the cyber operation constitutes an "attack" as soon as an intervention of the adversary is necessary to make the infrastructure or the system operational again (equipment repairs, replacement of parts, reinstallation of the network, etc.).

At this point it should be noted that Rule 92 of the *Tallinn Manual 2.0* is more nuanced than the French declaration portrays it to be. While it is true that the rule defines an attack through its physical effects on persons or property, it becomes clear from the commentaries that this is simply the minimum requirement all Experts could agree on. The Experts did intensively discuss whether interference with the functionality of an object constitutes damage or destruction for the purposes of Rule 92, with a majority supporting this view "if restoration of functionality requires replacement of physical components" (para. 10). Some Experts even held the view – now advanced by France – that if a computer system no longer can perform its intended function as a result of a cyber operation, this qualifies as damage (para. 11), rendering the cyber operation an attack within the meaning of Art. 49 AP I. It is a pity the authors of the declaration did not engage more extensively with the views expressed in the commentaries to Rule 92, as they did throughout the document with regard to other *Tallinn Manual 2.0* Rules.

This notwithstanding, it remains true that the French definition of a cyber "attack" seems to be the most expansive view articulated by a State to date. Most States have remained ambiguous or non-committal as to the definition of an "attack" in cyberspace. For instance, Australia "considers that, if a cyber operation rises to the same threshold as that of a kinetic 'attack under IHL', the rules governing such attacks during armed conflict will apply to those kinds of cyber operations," while the United States argue that "when determining whether a cyber activity constitutes an 'attack' for purposes of the law of armed conflict, States should consider, among other things, whether a cyber activity results in kinetic or non-kinetic effects, and the nature and scope of those effects, as well as the nature of the connection, if any, between the cyber activity and the particular armed conflict in question."

While the French expansive definition of an "attack" is fascinating from a legal point of view, its practical relevance in the current operational environment of the French armed forces may be limited. France asserts that most of the cyber operations carried out by its armed forces in the context of armed conflict (mainly the collection of information) do not meet the threshold of an "attack." In particular, France views the alteration of the adversary's propaganda capabilities by making a website unavailable through denial-of-service attacks as not governed by IHL by way of analogy to actions such as jamming of radio communications or of television programs, which cannot be characterized as an attack.

Conduct of Hostilities – the Principle of Distinction

> La France intègre les principes de distinction, de proportionnalité et de précaution à toute opération de lutte informatique offensive menée en contexte de conflit armé.
>
> France integrates the principles of distinction, of proportionality and precautionary measures to any offensive computer warfare conducted in the context of an armed conflict.

France affirms that by virtue of the principle of distinction, the parties to an armed conflict must distinguish between the civilian population and combatants as well as between civilian objects and military objectives (Art. 50-52 AP I). Accordingly, cyber attacks that are not directed against a military objective or whose effects may be indiscriminate are prohibited. In case of doubt about the status of persons or objects, they must be presumed civilian. In consequence, cyber operations have to be planned and coordinated in such a way that all practically possible measures are taken to verify that the targeted persons or objects are not civilian. If it is not established that the intended target is a military objective, the cyber operation has to be aborted.

In this regard, France takes issue with *Tallinn Manual 2.0* Rule 102, which states that "in case of doubt as to whether an object that is normally dedicated to civilian purposes is being used to make an effective contribution to military action, a determination that it is so may only be made following a careful assessment." In France's view, in cases of doubt as to the military character or use of an object, Art. 52(3) AP I is to be understood to require a presumption in favour of the civilian character of an object, rather than a further assessment, even if undertaken carefully.

However, it seems to me that the authors of the French declaration may have misunderstood the *Tallinn Manual 2.0* on this point. As para. 4 of the commentaries to Rule 102 makes clear, "[t]he sole issue addressed by this Rule is the standard for assessing whether a civilian object and its associated cyber infrastructure has been converted to military use." As I read it, Rule 102 therefore does not contradict Art. 52(3) AP I by suggesting different consequences in cases of doubt whether a civilian object is being used to make an effective contribution to military action, but rather sets out the necessary standard of care to be taken while making this determination.

> Les cyber-opérations visent exclusivement des infrastructures numériques identifiées comme objectifs militaires.
>
> Cyber operations may be aimed exclusively at digital infrastructures identified as military objectives.

With regard to the question what may constitute a military objective in cyberspace, in France's view military objectives may include ICT equipment or systems, data, processes or data streams (*flux d'échanges*) which compose a service, if they make an effective contribution to military action by their nature (*e.g.*, computer stations of the armed forces, command and control stations), location (*e.g.*, places from which cyberattacks are conducted), purpose (*e.g.* foreseeable use of computer networks for military purposes) or use (*e.g.*,use of a part of a network for military purposes) and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage (Art. 52(2) AP I).

It is interesting to note that France does not further discuss the question whether data can be regarded as an "object." While a majority of the *Tallinn Manual 2.0* Experts rejected this view arguing that data is intangible and therefore not included in the ordinary meaning of the word "object" (Rule 100, para. 6), France simply assumes that it is and proceeds to explaining under which conditions it might be regarded as a military objective. It therefore implicitly sides with the minority of the *Manual's* Experts, who argued (Rule 100, para. 7) that interpreting Art. 52 AP I with regard to its object and purpose requires to look at "the severity of the operation's consequences, not the nature of harm." In their view, targeting essential data such as bank accounts, tax records or social security information would eliminate the general protection from the effects of hostilities which civilians enjoy.

However, it seems to me that France comes to qualifying data as an object by another route. *First,* it is clear from the document that the starting point for any legal analysis, whether regarding peacetime law or *jus in bello*, is the nature of the cybersecurity incident caused by a cyber operation. France therefore looks not only at the secondary effects caused by the cyber operation, i.e. the physical effects on objects or people, but also at the primary effects on the targeted computer system with regard to breaches of information security principles (confidentiality, integrity, availability).

> En contexte de conflit armé, les cyber-armes visent principalement à produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité, l'intégrité ou la confidentialité des données.
>
> In the context of an armed conflict, cyber-weapons mainly aim to produce effects against an enemy system in order to alter its availability, integrity or confidentiality.

As a cybersecurity incident affects both the information systems and the data stored in them, operations targeting either of them carry legal consequences. This is, *secondly*, supported by the fact that our growing dependence on digitally-stored information includes more and more "virtual objects" (my descriptive term, not used by France) in the necessities of daily life. This becomes apparent in France's view that civilian content data is protected by the principle of distinction (and therefore implying that data is an "object").

> Au regard de la dépendance numérique actuelle, des données de contenu (comme des données civiles, des données bancaires, des données médicales etc.) sont protégées au titre du principe de distinction.
>
> In view of the current digital dependency, content data (such as civilian data, bank data, medical data, etc.) are protected under the principle of distinction.

In consequence, objects, including data, which do not fulfil the criteria mentioned above, have to be considered civilian objects and must not be attacked. In particular, it is prohibited to conduct attacks through cyberspace against computer systems in schools, hospitals and other medical facilities, as well as other exclusively civilian services. Data of a civilian nature (bank data, medical data etc.) must also not be attacked. Dual-use computer infrastructure may be targeted if, as a result of a case-by-case analysis, it is to be considered a military objective. Nevertheless, due to the

interconnectedness of dual-use systems, precautions have to be made and the principle of proportionality has to be observed in order to reduce to a minimum the effects on civilian objects.

Cyber-combatants, including military personnel assigned to a cyberspace operations command, a state-controlled group of hackers or members of organized armed groups conducting cyberattacks against the adversary, may be attacked unless they are *hors de combat*. Every other person is considered a civilian and enjoys protection against the dangers arising from military operations, unless he participates directly in hostilities. The conduct of a cyber operation intended to harm the military operations or military capability of a party to an armed conflict to the detriment of that party and to the advantage of an adverse party, or which is likely to cause loss of life, injury or damage of a civilian nature, may constitute a direct participation in hostilities.

Conduct of Hostilities – the Principles of Precaution and Proportionality

France reaffirms Art. 57 and 58 AP I, which require a party to the armed conflict to take constant care in the conduct of military operations to spare the civilian population, civilians and civilian objects. Despite the adoption of the necessary precautions, if the neutralization or the destruction of a military objective by cyber means is likely to generate civilian damages, these must not exceed the direct and concrete military advantage expected. The risks inherent in cyberspace (immediacy of effects, intrinsic duality of military objectives, interconnectedness, low traceability of operations, vulnerability of civilian systems) must thus be taken into account in order to determine the modes of action and the means to be implemented in the field to ensure compliance with the principle of proportionality.

Furthermore, the principles of precaution and proportionality require special care in the development and use of cyber weapons. Although the expected effect of a cyber weapon may be difficult to measure, the risk of spreading the effects of a cyber weapon beyond the intended target should be controlled through the development of use-specific cyber weapons, which would be activated only if certain conditions are met (*e.g.* activation of malware only in previously identified networks, existence of a delay function, etc.). The use of malicious programs that reproduce and spread without control or reversibility and are thus likely to cause significant damage to critical civilian systems or infrastructure, is contrary to IHL.

The evaluation of the effects of a cyber operation takes into account all the foreseeable direct and indirect damage likely to be caused by the cyber weapon. Direct damage may include damage to the computer system or interruption of the system, while indirect damage may include effects on infrastructure controlled by the system, affected by the malfunction or destruction of the targeted system or by the alteration and corruption of data contained in the system.

Neutrality in Cyberspace

France reiterates the view that the law of neutrality applies to cyber operations conducted as part of an international armed conflict. In consequence, States parties to the armed conflict may neither conduct cyber operations related to this conflict from facilities located in the territory of, or under the exclusive control of, a neutral State, nor may they take control of the neutral State's computer systems to conduct such operations.

For its part, the neutral state must prevent any use of ICT infrastructure located on its territory or under its exclusive control by belligerent States. Nevertheless, it is not obliged to prevent them from using its computer networks for communication purposes. The fact of routing a cyber operation constituting an attack via the systems of a neutral State without any effect on it does not constitute a violation of the right of neutrality, which only prohibits the physical passage of troops or convoys.

Summing up, it has to be said that France's declaration of "International Law Applicable to Operations in Cyberspace" is undoubtedly the result of a long and detailed analytical process, which undoubtedly will advance the discussion on j*us ad bellum* and j*us in bello* in cyberspace. It remains to be hoped that France will translate the document into English as soon as possible so that it may be widely disseminated and receive the attention it clearly deserves.

About the Author(s)

Przemysław Roguski

Dr. Przemysław Roguski is a Lecturer in Law at the Jagiellonian University in Kraków (Poland) and an expert on cybersecurity and international law at the Kościuszko Institute. Follow him on Twitter (@Roguski_P).