GENEVA ACADEMY

Académie de droit international humanitaire et de droits humains

Academy of International Humanitarian Law and Human Rights

RESEARCH BRIEF

PROTECTION OF DATA IN ARMED CONFLICT

FEBRUARY 2021 I ROBIN GEISS AND HENNING LAHMANN

THE GENEVA ACADEMY A JOINT CENTER OF

THE GRADUATE INSTITUTE GENEVA

INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT

GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES

UNIVERSITÉ DE GENÈVE

FACULTY OF LAW

INTRODUCTION

These days, our thoroughly digitalised societies run on data. Indeed, the notion of data is embedded in the very concept of digitalisation, and no process or service that relies on computing power is conceivable without it. It is therefore only natural that experts of international humanitarian law (IHL) have for a while now pondered over the question of how to treat data under the existing legal frameworks applicable to armed conflicts, starting from the premise that military operations affecting data 'could cause more harm to civilians than the destruction of physical objects'.[1] At the same time, the debate has at times suffered from ambiguities and inaccuracies concerning the subject matter. The present paper attempts to clarify some of the involved concepts and lays out the problem by exposing the relevance of the protection of data in armed conflict, based on a number of brief scenarios. After summarising the present debate relating to the application of the rules of armed conflict, the paper goes beyond the limited scope of existing IHL in order to advance awareness of the problem as a starting point for further discussion.

MAPPING THE THREAT LANDSCAPE: DATA RISKS IN CONTEMPORARY ARMED CONFLICT

Military cyber operations can affect civilian data in different ways, depending on the means of conduct and the operation's target. In the following, a few scenarios shall make clear what is potentially at stake.

SCENARIO A – RANSOMWARE OPERATION AGAINST A HOSPITAL

During a situation of armed conflict, the military of State A carries out a ransomware operation against the servers of a major hospital in State B that store the patients' case files, encrypting them until State A is willing to withdraw its troops from a contested island located on the continental shelf of State B. No patient suffers physical harm, but a great number of surgeries and other essential medical treatments have to be postponed, and a couple of persons need to be transferred to other hospitals.

In a variation of this scenario, the operation is only seemingly a ransomware attack. In fact, the military of State A employs a wiper malware, which immediately leads to the destruction of all patient files on the affected server, requiring hospital staff to recreate the files on paper from scratch.

SCENARIO B – FINANCIAL DAMAGE THROUGH DATA LEAKS

A few days before the company's initial public offering (IPO) at the national stock exchange, the military of State B launches a cyber operation against the IT systems of Company C, which is headquartered in State A. The two states have been engaged in an armed conflict for the past year. The military cyber unit extracts a large file containing sensitive business data that expose a financial scandal involving the leadership of Company C, the CEO of the national stock exchange, and the heads of the national financial supervision authority. State B subsequently leaks the data through a non-governmental organisation that specialises in exposing classified information and other secrets. As a result, the IPO of Company C is cancelled and the stock market crashes, which leads to considerable economic damage and to a sustained rise in unemployment in State A.

SCENARIO C – CYBER OPERATION AGAINST WATER TREATMENT FACILITY

During a situation of armed conflict, the military of State A engages in an offensive cyber operation against the industrial control systems (ICS) of a water treatment facility in State B, altering critical datasets essential for the maintenance of the correct level and mixture of chemicals for processing the drinking water for a major city. As employees notice the tampering, they carry out an emergency shutdown of the facility, which leads to minor water shortages in the city for three days.

SCENARIO D – DATA COLLECTION AND RELEASE 3.0

Exploiting a vulnerability in one of the servers of Company C, the major state-owned petroleum and natural gas company in State A, a religious and socially conservative country is in a protracted situation of armed conflict with State B, the latter's military cyber unit deploys the Mimikatz tool in order to obtain the passwords of the company's employees. Using the stolen password of one of the executives, the military hackers manage to extract terabytes of unencrypted emails and the social security numbers from employees that contain both business and private information. Among other things, a number of emails reveal intimate facts such as the homosexuality of a couple of employees, which is a felony punishable by imprisonment in State A. Pretending to be citizens of

1 International Committee of the Red Cross, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (*ICRC Report*, 31 October 2015) ‹https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts› accessed 26 January 2021, 43

State A that belong to an organisation concerned with 'religious purity', service members of the cyber unit leak the sensitive information to major newspapers in State A who subsequently publish stories about the respective employees, leading to criminal indictments and death threats. State B's military furthermore sells the obtained social security numbers on the dark web.

SCENARIO E – DIGITAL BLACKMAIL

After a year of armed hostilities between States A and B, the military of State B hacks the IT systems of the largest cellphone and internet provider of State A. The hackers extract a large trove of data, among them the location data and call records of all customers. They also use the company's networks to secretly install surveillance software in one of the country's main internet exchange points, allowing State B to subsequently monitor the data traffic in State A in real time. The analysis of the phone and internet metadata reveals inter alia that member of parliament M, who belongs to the ruling party in State A, has been having an extramarital affair. The military of State B uses that information to coerce M into voting against a parliamentary act that would have significantly increased troop presence on the border between the two countries.

THE QUALIFICATION AND PROTECTION OF DATA UNDER EXISTING LEGAL FRAMEWORKS

CONCEPTUAL EXPLICATIONS

Before commencing with the application of black-letter law to cyber operations against 'data' in armed conflict, a couple of notional clarifications are in order. The first and most important is the concept of 'data' itself. In its most general sense, computer data is

'information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data. Computer data may be processed by the computer's CPU and is stored in files and folders on the computer's hard disk. At its most rudimentary level, computer data is a bunch of ones and zeros, known as binary data. Because all computer data is in binary format, it can be created, processed, saved, and stored digitally. This allows data to be transferred from one computer to another using a network connection or various media devices. It also does not deteriorate over time or lose quality after being used multiple times.'[2]

In other words, the entirety of the 'raw material' needed by computer systems to function can be described as data. This is crucial and at times poorly understood by legal scholars or policy-makers who try to grapple with the legal implications of 'attacking data', as the unspoken focus is often on data that represents information that can be read, viewed, heard, or otherwise sensually consumed by humans, but not on data that carries information solely to be processed by computing units. This distinction on the factual level is important as it needs to be clarified what is meant when we talk about 'data protection' in armed conflict. One of the few scholars to make this clear and to take it as the starting point of her inquiry is Dinniss, who proposes two separate categories of data supposedly relevant for the legal analysis: On the one hand, there is *content-level data*, 'such as the text of this article, or the contents of medical databases, library catalogues and the like';[3] thus, this is data that represents information which, after being processed, is in principle intelligible to humans, for example when displayed on a computer screen. *Operational-level data*, on the other hand, 'also known as logical-level data or, more commonly, program data ... gives hardware its functionality and ability to perform the tasks we require. Operating systems, software applications and SCADA systems are all examples of operational-level data'.[4] This category of data, which consists of machine-readable commands, is more commonly referred to as 'code', as noted by Dinniss. Crucially for the following legal analysis, her examination is almost entirely focused on the second category, as she considers content-level data, with few exceptions, outside the scope of the applicable law of armed conflict. Most other scholars tackle the question of whether and in which way IHL protects content-level data when explicitly talking about 'data protection' in armed conflict.

A further distinction between different kinds of computer data that is not to be confused with the categories proposed by Dinniss is that between content data on the one hand and metadata on the other. The latter is data about data, i.e. data that summarizes basic information about data, such as author, date created, or file size.[5] For example, while the text of an email is its content, the timestamp, information about its size in kilobytes, and perhaps the geolocation of its sender (especially if dispatched via a mobile device) is the

2 Per Christensson, 'Data Definition' (*TechTerms* 2006) ‹https://techterms.com/definition/data› accessed 27 August 2020

3 Heather Harrisson Dinniss, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives' (2015) 48 Israel Law Review 39, 41

4 ibid

5 Margaret Rouse, 'Definition: Metadata' (*TechTarget* December 2019) ‹https://whatis.techtarget.com/definition/metadata› accessed 26 January 2021

email's metadata. Importantly, metadata is not 'code'; the information expressed is intelligible to humans. In Dinniss' understanding, both the email's content and its metadata thus count as 'content-level data'.

These factual-definitional distinctions of data are complemented by a normative dimension: the differentiation between personal and non-personal data. The distinction lies at the foundation of modern data protection frameworks such as the European General Data Protection Regulation (GDPR). Personal data is 'any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data'.[6] While 'operational-level data', as understood by Dinniss, will almost by default not fall within the scope of personal data, 'content-level data', both content information itself and metadata, frequently will, although it is important to understand that this need not necessarily be the case. The content of an email that conveys the information that the sender is getting married next week is personal data, whereas content that merely makes a statement about the weather (usually) is not.

Strictly speaking, the protection of data in armed conflict is concerned not with 'data protection' in the common legal sense, which is the body of law that regulates how personal data may be processed by persons and entities who control that data,[7] but with 'data security', which is part of the rules on data protection[8] but conceptually belongs to information/IT security more generally. The key concepts of data/information security, which are highly relevant for the matter at hand but not always sufficiently spelled out in this context, are the confidentiality, integrity, and availability of the IT systems that process the data and thus of the data itself. 'Confidentiality' means that data and the system on which it is stored is protected from unauthorised access in order to prevent misuse of the data. It is closely related to and a precondition of privacy. Online surveillance measures or the extraction of data by way of electronic espionage operations affect the confidentiality of data. 'Integrity' of data refers to the maintaining and assuring of the accuracy and completeness of stored data. Adversarial cyber operations that delete targeted data, for example by means of a wiper malware, or that manipulate data in order to alter the outcome of a certain computing process, as in the case of Stuxnet, concern the integrity of data. Finally, 'availability' of data means that the stored information is accessible and processable whenever needed or desired. A DDoS attack that leads to a crashing of the targeted IT system affects the availability of the data located on that system for as long as the operation lasts. A ransomware that encrypts all data stored on a system's hard drive is also an operation against the availability of that data. When assessing military cyber operations in the context of armed conflicts, referring to the three basic concepts of information security adds analytical clarity, as different rules may apply and different legal consequences may follow depending on which protective goal is concerned.

INTERNATIONAL HUMANITARIAN LAW

Depending on what category of data is being examined, the analysis of legal protections under IHL will differ. Taking Dinniss' fundamental distinction as a starting point, the emphasis of the following survey of the existing law will be on content-level data, for reasons that will be explained.

Conduct targeting operational-level data (code) – the 'standard type' of cyber operations

Adversarial cyber operations that target either the availability or the integrity of operational-level data 'will result in loss of functionality of the system'.[9] However, understood in this way, the 'object of attack' of such an operation is not the data as such but the affected system itself, as correctly pointed out by Schmitt.[10] Indeed, in the physical world we are also not thinking of an attack as an attack against the atoms and molecules forming an object, but of an attack against their sum-total, i.e. the object as such. If all software code is conceived of as 'data', as Dinniss put forward – which is correct from a purely technical point of view – then virtually every type of cyber operation, with very few exceptions (e.g. some variations of so-called side-channel attacks), by definition targets (operational-level) data: altering, adding, rewriting, corrupting or otherwise manipulating lines of *code* – i.e., data – by means of introducing code, i.e. data (viruses, worms, trojan horses, rootkits, etc.). Therefore, in order to assess what rules of existing IHL might apply and whether the operation would be prohibited due to a violation of the principle of distinction (Article 48(1) AP I), the principle

6 European Commission, 'What Is Personal Data?' ‹https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en› accessed 26 January 2021

7 See e.g. Art 1(1) Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and repealing Directive 96/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 (hereafter GDPR)

8 See e.g. Art 32 GDPR

9 Dinniss (n 3) 42

10 Michael N Schmitt, 'The Notion of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision' (2015) 48 Israel Law Review 81, 104-5

of proportionality (Article 51(5)(b) AP I), or of the duty of precautions in attack (Article 57 AP I), one needs to look at the consequences of the operation. In other words, this is the standard debate concerning the qualification of military cyber operations under the laws of armed conflict, as dealt with exhaustively in both academic literature and official legal statements by states.

Conduct targeting content-level data – a legal grey zone under IHL

This leaves the issue of the application of the rules of IHL to cyber operations that target content-level data. As observed by Dinniss, an operation that affects the integrity of stored data itself 'will leave the system intact, albeit with corrupted or missing data'.[11] Operations against the availability of data will have no effect on the data itself but thwart its availability, although it can be argued that encrypting the data in a ransomware attack, even if the key to decrypt it exists, is actually directed against its integrity and not simply its availability. Military cyber conduct that targets the confidentiality of data will, unless something unforeseen happens, harm neither the system itself nor the stored data, but merely make a copy of the latter. To date, the debate among experts and state representatives as to the applicability of IHL to cyber operations against data directly has focused on conduct that compromises the integrity of data, as '[d]eleting or tampering with [essential civilian data] could quickly bring government services and private businesses to a complete standstill, and could cause more harm to civilians than the destruction of physical objects'.[12]

Special legal protections for certain categories of data

Certain civilian infrastructures enjoy specific protection under IHL, including, most importantly, medical services and infrastructures, which 'must be respected and protected by the parties to the conflict at all times'.[13] Due to this broad and unqualified scope, there is general agreement that this protection comprises personal medical data,[14] for example patient records or other information relating to individuals in treatment, as well as any other data 'belonging to medical units and their personnel'.[15] This position has been expressed by states that have made statements on the application of international law to cyber operations, most recently explicitly France.[16] Furthermore, as cyber operations that target objects indispensable for the survival of the civilian population are prohibited, data necessary for the functioning of these especially protected objects and services is protected as well, as also observed by France.[17] Thus, the targeting of medical data stored on hospital servers, as in Scenario A, is prohibited irrespective of the consequences of the operation.

Other content-level data

The protection under IHL of data not necessary for medical or other indispensable civilian services against adversarial cyber operations has been a contentious and to date mostly unsettled issue. This is because although the foundational principle of distinction stipulates that the parties to an armed conflict must at all times distinguish between civilian objects and military objectives, which means that '[a]ttacks shall be limited strictly to military objectives' according to Article 52(2) AP I, the provision defines 'military objectives' as follows:

> 'In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.'

Consequently, there is general agreement among experts that targets of adversarial military cyber operations in armed conflict that are not 'objects' are not protected by the principle of distinction and other rules of IHL that regulate targeting.[18] Therefore, it needs to be clarified whether data by itself can be considered an object for the purpose of IHL. If not, cyber operations that do not affect the targeted IT systems and do not lead to physical consequences but only

11 Dinniss (n 3) 42

12 International Committee of the Red Cross (n 1) 43

13 Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser, 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong Are International Law Protections?' (*Just Security*, 27 March 2020) ‹https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/› accessed 26 January 2021

14 See Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) (hereinafter Tallinn Manual) rule 132 para 3

15 Mačák, Gisel and Rodenhäuser (n 13)

16 Ministère des Armées de France, 'Droit International Appliqué Aux Opérations Dans Le Cyberspace' (2019) ‹https://www.defense.gouv.fr/content/download/565896/9750885/file/Droit+internat+appliqué+aux+opérations+Cyberespace+-+résumé.pdf› accessed 26 January 2021, 15

17 See Michael N Schmitt, 'France Speaks out on IHL and Cyber Operations: Part II' (*EJIL Talk!*, 1 October 2019) ‹https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/› accessed 26 January 2021

18 Michael N Schmitt, 'International Cyber Norms: Reflections on the Path Ahead' (2018) 111 Militair Rechtelijk Tijdschrift 12 ‹https://puc.overheid.nl/mrt/doc/PUC24813711/› accessed 26 January 2021

have effects on the integrity of data itself, as in the above scenarios B, D, and E, would not fall under the ambit of the principle of distinction and other rules on targeting and would thus not or only minimally be protected in situations of armed conflict.

The ongoing debate about the question of whether data has object-quality for the purpose of IHL comes down to two main positions. Proponents of the first view contend that the notion of 'object' in Article 52(2) AP I, taking its ordinary meaning, implies that the target of the military operation must be an entity of a physical quality, i.e. be something that is visible and tangible in the real world.[19] This argument is supposedly supported by the 1987 ICRC Commentary to the Additional Protocols and mainly rests on a very literal understanding of 'object'. Data, as something invisible and intangible by definition, can therefore not be conceived as an object for the purpose of IHL. Only if the cyber operation targeting stored data subsequently and directly leads to physical effects on a physical object, as in scenario C above, the principle of distinction and other relevant rules of the laws of armed conflict apply.[20] Furthermore, it has been put forward that treating data as objects would considerably curtail the options belligerent states would have in armed conflict to act against their adversary. Given that the deletion or manipulation of data might provide a convenient – and potentially less lethal or destructive – route to subdue the enemy,[21] states would likely not accept an expansive interpretation of the notion of 'object' that would include data *per se*.[22]

The opposing position holds that data can indeed be subsumed under the notion of 'object'. The 1987 ICRC Commentary, which seems to suggest the visibility and tangibility as a necessary precondition of object-quality, did in fact not at all address the question of data – having been drafted and published before the digital transformation – but merely sought to clarify that only concrete things are subject to the principle of distinction and other rules, but not purely abstract concepts such as, for example, 'civilian morale'. Considering this binary distinction, data was clearly notionally more akin to concrete things, given that it can be targeted and destroyed in a similar way as a military would attack a building or an enemy's weapon system. Morale, on the other hand, is a purely subjective category that might be affected by an attack, but can hardly be targeted as such.[23] Apart from this textual and contextual reading of Article 52 AP I, proponents of this view additionally invoke a teleological consideration. As Additional Protocol I generally aims at improving the protection of victims of armed conflict, and Part IV of AP I, of which the rules under scrutiny form a part, deals with civilians as a subcategory of victims of armed conflict in particular, it follows that 'the object and purpose of Article 52(2) and its normative context is the enhancement of the protection of civilians during situations of armed conflict'.[24] In light of this, a restrictive literal interpretation of 'data' would have the consequence that 'many targets whose physical equivalents are firmly protected by IHL from enemy combat action would be considered fair game as long as the effects of the attack remain confined to cyberspace',[25] leading to a critical protection gap.[26] This runs counter to the very rationale of this body of law and must thus be rejected on this basis.[27] For these reasons, data should be accepted as 'object' in the context of military operations. Thus, the pertinent rules apply, which means that in the case that the data is to be qualified as a civilian object, it enjoys the protections of IHL. Emphasising the premise that societies have become too reliant on data to exclude it from the specific protections of IHL, France has recently explicitly endorsed this position.[28]

At the same time, if data is considered an object, it would additionally need to be assessed whether the military cyber operation could be considered an 'attack' for the principal rules on targeting to be triggered, such as the rule of proportionality or the rule on precautions in attack. In this context, it has been pointed out that as soon as the object-quality of data is accepted, operations that aim at affecting the integrity of data would necessarily qualify as attacks given that 'damage and destruction are conditions precedent to qualification as an attack'.[29] This argumentation also implies that military conduct that leaves the data itself intact, such as espionage or surveillance operations that are merely directed against the confidentiality of data, would

19 Michael N Schmitt, 'Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations' (2019) 101 International Review of the Red Cross 333, 340

20 See Schmitt (n 18)

21 Schmitt (n 19) 342

22 Michael N Schmitt, 'The Law of Cyber Warfare: Quo Vadis?' (2014) 25 Stanford Law & Policy Review 269, 298

23 Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 Israel Law Review 55, 73

24 ibid 78

25 ibid

26 International Committee of the Red Cross, 'International Humanitarian Law and Cyber Operations During Armed Conflicts' (*ICRC Position Paper*, 28 November 2019) ‹https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts› accessed 26 January 2021, 8

27 International Committee of the Red Cross (n 1) 43

28 Ministère des Armées de France (n 16) 15

29 Schmitt (n 10) 95

not count as an attack for the purpose of IHL.[30] In light of this, it is unclear how to qualify operations that target the availability of data, such as a DDoS attack; Schmitt suggests that 'simply blocking data transmission'[31] would not suffice. However, again, this assessment only holds true in regard to data that does not belong to a specially protected category, as the medical data that was targeted in above scenario A.

INTERNATIONAL HUMAN RIGHTS LAW AND DATA PROTECTION FRAMEWORKS

Many essential civilian data sets that could potentially be affected by adversarial military cyber operations in situations of armed conflict that aim at disrupting societal functions on the territory of their enemy fall into the category of personal data as defined above – examples that have been mentioned include 'civil registries, insurance data, medical data',[32] 'social security data, tax records, and bank accounts'.[33] Thus, *prima facie,* such data would be subject to the scope of data protection frameworks such as the GDPR. However, Article 2(2) GDPR clarifies that its provisions apply neither to 'issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security' nor to 'the processing of personal data by Member States when carrying out activities in relation to the common foreign and security policy of the Union'.[34] This limitation would seem to preclude the application of this legislation from any state activities in relation to conduct during situations of armed conflict. To be sure, the fact that a state is party to an armed conflict does not relieve data controllers[35] or data processors,[36] such as the banks, insurances, hospitals, or public administration officials that are in possession of and handle essential personal data of their customers and citizens, of their duties under data protection frameworks such as the GDPR, where applicable. This includes the obligation to implement measures 'to ensure a level of security [of the stored data] appropriate to the risk'.[37]

Furthermore, contemporary data protection frameworks are, conceptually speaking, legislative substantiations of the human right to privacy. In light of this, it does seem worthwhile to ask whether this right might be applicable in situations of armed conflict alongside the rules of IHL to adversarial cyber operations. This requires an examination of the relationship between IHL and international human rights law on the one hand,[38] and of the application of human rights treaties to extraterritorial ('virtual') situations on the other.[39] In the wake of the revelations regarding the extensive global online surveillance activity of U.S. and British intelligence services by Edward Snowden in 2013, Milanovic advocated for a more expansive application of the right to privacy in order to reflect state conduct after the digital transformation.[40] However, it should be noted that these deliberations concerned peacetime conduct and were limited to surveillance, which only tackles one aspect of operations targeting the confidentiality of data, not their integrity or availability.

INHERENT LIMITATIONS OF EXISTING APPLICABLE LAW: ADVANCING THE DEBATE

As has been demonstrated in the foregoing sections, the debate revolving around the question of the protection of data in armed conflict at times suffers from conceptual confusion and definitional ambiguities concerning the notion of 'data' itself. This discussion paper has attempted to offer some clarification. At its broadest and at the same time most basic understanding, almost every type of cyber operation is by definition targeting data. The inherent difficulties with trying to capture this foundational insight of cybersecurity within the existing rules of international law, including IHL, were eventually resolved by way of focusing on the consequences of cyber operations for the purpose of legal assessment (effects- or consequence-based approach).[41] At the same time, this discussion is inherently limited as it does not address the question what rules, if any, apply to cyber operations that are directed against data that merely represent information, i.e. the targeting of which does not have any physical effects at all.

30 ibid 101

31 ibid 105

32 Laurent Gisel and Tilman Rodenhäuser, 'Cyber Operations and International Humanitarian Law: Five Key Points' (*Humanitarian Law & Policy*, 28 November 2019) ‹https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/› accessed 26 January 2021

33 Schmitt (n 19) 340

34 Recital 16 GDPR

35 See for the definition Art 4(7) GDPR

36 See for the definition Art 4(8) GDPR

37 See Art 32(1) GDPR

38 See only Janina Dill, 'Towards a Moral Division of Labour between IHL and IHRL during the Conduct of Hostilities' in Ziv Bohrer, Janina Dill and Helen Duffy (eds), *Law Applicable to Armed Conflict* (Cambridge University Press 2020) 197

39 ee only Helen McDermott, 'Application of the International Human Rights Law Framework in Cyber Space' in Dapo Akande, Jaako Kuosmanen, Helen McDermott and Dominic Roser (eds), Human Rights and 2*1st Century Challenges: Poverty, Conflict, and the Environment* (Oxford University Press 2020) 190

40 Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2014) 56 Harvard International Law Journal 81

41 See only Schmitt (n 10) 97

Therefore, the debate must go beyond what Dinniss calls 'operational-level data' and focus on 'content-level data', i.e. the protection of stored data in and of itself, which includes both what is commonly called 'content' as well as metadata. Here, the ongoing debate among experts and policy-makers has revealed the inherent limitations of existing IHL, which at its core is concerned with the *physical effects* of armed conflict. As a consequence, then, existing protections at most encompass cyber operations against the availability or the integrity of data, but *only* if they entail physical or otherwise tangible harmful consequences – as shown in scenarios B, D, and E. Operations against the confidentiality of data, for example in the context of surveillance or espionage, but also for the purpose of misusing personal data in order to coerce or otherwise influence the behaviour of individuals in situations of armed conflict (scenarios D and E), are outside the scope of existing IHL unless they fall into a specially protected category of data, as in scenario A.[42]

In light of this, it is submitted that these inherent limitations call for a prospective discussion that transcends the purely ontological inquiries revolving around the object-quality of computer data that have dominated the discourse so far. Given the significance of data for modern digitalised societies, one might propose a paradigm shift: To date, as was shown, the prevalent debate has taken the rules and principles of existing IHL (in particular the notions of 'object' and 'attack') and applied them to 'data'. A different and novel approach would be to take, as a starting point, the principles of existing data protection, data security, and other pertinent legal frameworks and attempt to apply them to contemporary armed conflict. Such an approach might be better suited to accommodate the actual relevance of data for the information society and to address the resultant protection needs during armed conflict.

In reversing the direction of consideration, the leading question then becomes: *Should* certain types of data enjoy protection from adversarial cyber operations in armed conflict, *irrespective of* whether data qualifies as an 'object' or not? If this is accepted in principle, a number of different dimensions of 'data protection' in armed conflict could be taken into account:

(1) Should operations against the *availability* of civilian data be restricted even if they do not cause harmful (physical) consequences?

(2) Should operations against the *integrity* of civilian data be restricted even if they do not cause harmful (physical) consequences?

(3) Can operations against the *confidentiality* of civilian data be restricted?

As these questions imply, securing the confidentiality of personal data – one of the core principles of existing data protection frameworks – is mostly outside the scope of what has so far been considered to require or deserve protection during armed conflict. However, the harm to individual civilians could nevertheless be significant, even if the harm is not *physical.* As repeatedly confirmed by domestic courts around the world, the right to privacy – 'the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others'[43] – is based on and serves as a protection of the dignity of a person. A complete collapse of privacy during armed conflict as a consequence of adversarial military cyber operations would be a paradigm shift of how wars are fought and could in principle conceivably lead to a paralysis of the targeted civilian society at large.

As a starting point for discussion, the possible protection of the confidentiality of (personal) civilian data could approach the question in relation to two different aspects. First, one might focus on the properties of the data itself and ask whether there are certain types of civilian data that should enjoy increased protection in and of themselves. For example, the GDPR acknowledges 'special categories of personal data' that are, 'by their nature, particularly sensitive in relation to fundamental rights and freedoms' and thus 'merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms'.[44] These properties include 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership' as well as 'genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.[45] It seems doubtful that these 'special categories of data' would lose any of their sensitivity during armed conflict. Second, the discussion should zoom in on a possible regulation of what adversarial states who obtain civilian data by way of conducting military cyber operations in armed conflict are permitted to do with that

42 See Mačak (n 23) 74

43 Federal Constitutional Court of Germany, BVerfG 65, 1 (15 December 1983)

44 Recital 51 GDPR

45 Art 9(1) GDPR

data (or with different categories of personal civilian data). For example, while it is inconceivable to establish a blanket prohibition of surveillance and espionage activities, one might contemplate a rule against certain specified uses of the collected data such as publishing or leaking sensitive personal data and/or a rule against exploiting such data sets for the purpose of coercion, extortion, or manipulation. Not least with the increasing use of artificial in military decision making, states will be ever more inclined to obtain a full take of all data relevant to a given theatre of combat. Discussing restrictions regarding particularly harmful uses of such data will therefore become increasingly relevant.

CONCLUSIONS

As the paper has shown, so far the question of the protection of 'data' in situations of armed conflict has been discussed from the angle of its object-quality, which would make the concept more readily fit the existing body of IHL. While this endeavour is worthwhile, the different ways data – and the information it represents as well as the attached rights and interests of individuals and societies it incorporates – can be affected by cyber operations might require us to look beyond this traditional scope and instead consider what kind of approach will be necessary to grasp and adequately protect the various functions of data in our digitalised societies that depend (at least on a minimum) of confidentiality, integrity, and availability of both personal and non-personal data. With this in mind, the paper has attempted to lay out some initial considerations and questions in order to serve as a conversation starter.

THE GENEVA ACADEMY

The Geneva Academy provides post-graduate education, conducts academic legal research and policy studies, and organizes training courses and expert meetings. We concentrate on branches of international law that relate to situations of armed conflict, protracted violence, and human rights protection.

DISRUPTIVE MILITARY TECHNOLOGIES

New (military) technologies are set to revolutionize the ways wars are fought. This research project aims at staying abreast of the various military technology trends; promoting legal and policy debate on new military technologies; and urthering the understanding of the convergent effects of different technological trends shaping the digital battlefield of the future.

The Geneva Academy
of International Humanitarian Law
and Human Rights

Villa Moynier
Rue de Lausanne 120B
CP 1063 - 1211 Geneva 1 - Switzerland
Phone: +41 (22) 908 44 83
Email: info@geneva-academy.ch
www.geneva-academy.ch