INTERNATIONAL LAW STUDIES

Published Since 1895

International Humanitarian Law and the Targeting of Data

Tim McCormack

94 INT'L L. STUD. 222 (2018)

Volume 94 2018

Stockton Center for International Law, U.S. Naval War College

ISSN 2375-2831

International Humanitarian Law and the Targeting of Data

Tim McCormack[*]

CONTENTS

I. Introduction 223
II. International Humanitarian Law and Cyber Attacks 224
III. The Increasing Significance of Data and the Deleterious Impact of Cyber Operations 234
IV. Is Data an Object for the Purposes of the Application of International Humanitarian Law? 237
V. Conclusion 239

[*] Tim McCormack is Dean of the University of Tasmania Law School and a Professorial Fellow at Melbourne Law School. He is also the Special Adviser on International Humanitarian Law to the Prosecutor of the International Criminal Court, the Department of Foreign Affairs and Trade's Visiting Legal Fellow (appointed jointly with Professor Anthea Roberts 2017–18), and the New Zealand Law Foundation Distinguished Visiting Fellow (2018). Previously, he served as the Charles H. Stockton Distinguished Scholar-in-Residence at the U.S. Naval War College (2015–16) and as a member of the International Group of Experts that drafted *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2015–17). None of the views expressed in this article can be attributed to any of the institutions named above. Professor McCormack wishes to thank Luke Chircop for his helpful research assistance in the preparation of this article and Professor Rob McLaughlin for his insightful comments on the topic, particularly in a presentation to Australian Defence Force Legal Officers in Canberra on August 30, 2018. An earlier version of this paper was presented at "Future Wars and Public Conscience: Symposium on the Ethical, Legal and Social Implications of Emerging Military Technologies" in Melbourne, Australia, May 29–30, 2017.

The thoughts and opinions expressed are those of the author and not necessarily those of the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.

I. INTRODUCTION

On a basic level, digital data is composed of a complex succession of 1s and 0s. As I key in this very sentence, my software accurately processes the otherwise unreadable data into the words that I am composing. A printed copy of my software-processed data is of course a tangible object—we speak in terms of "hard" and "soft" copy to distinguish physical from virtual. Some of us from earlier generations, myself included, still prefer to move from soft to hard copy and back again, but it is impossible to function in a contemporary industrialized economy without recognizing the sheer ubiquity of digital data. Even that small minority of the population that does not own a smartphone or have any online presence in social media is still likely to use email, watch television, possess a debit or credit card for financial transactions, own a passport, visit a medical professional, use public services or facilities, attend school, drive a motor vehicle, use public transport, use electricity from a grid, use running water from a connected supply, or walk in a public space and be filmed on closed-circuit television. A twenty-first century human life isolated from electronic data is an increasing rarity.

The technicalities of the electronic composition of data and the ubiquity of its presence in twenty-first century life does not capture the full significance of personal data. My ability to key in text is, of course, a consequence of the development of word processing, but I also want to preserve my intellectual property in the sentences that I construct. My thought processes that lead to the selection of keys in the construction of words is my intangible property. Another person's appropriation of my intellectual property without attribution constitutes plagiarism—and that is an offense in academic circles where we rightfully expect that the work a professor or a student puts his or her own name to is indeed his or her own—unless attribution to others' work is duly made. My legal entitlement to the integrity of the authorship of my self-generated data is reflective of widespread and popular acceptance that data is more than a complex succession of 1s and 0s. And it is not the case that intellectual property in one's self-generated data is the full extent of our sense of proprietorial interest. Personal data, including home address, investment portfolio details, passport details, social security number, credit card and personal banking details, personal health records, and so forth include the sorts of information few of us want freely available to the public.

In a recent article in *The Economist*, the editorial staff explores the emerging argument that people should be paid for their personal data.[1] Given that corporate entities are already prepared to pay for data supplied by technology firms, why not cut out the intermediaries and allow individuals to sell their own data if they choose to do so? The Cambridge Analytica debacle, which resulted in the acquisition of the personal data of 87 million Facebook users without the consent or knowledge of those users, has sharpened focus on this issue.[2] Even Angela Merkel, the German Chancellor, has challenged researchers to quantify the economic value of personal data.[3] In our digitally connected world, personal data has become an important commodity.

II. INTERNATIONAL HUMANITARIAN LAW AND CYBER ATTACKS

Academic scholarship and popular literature tends to describe all known offensive cyber operations generically as "attacks."[4] Accordingly, legal scholars such as Noam Lubell lament the popular misuse of the term "attack" to describe all offensive cyber operations because of the legal uncertainty that the misuse of the term creates.[5] Thus, he argues: "For the sake of legal clarity, it would therefore be advisable to utilize a more legally neutral (at least under the *jus in bello*) description and—unless intending to define an event as an attack under LOAC—to speak of cyber operations rather than cyber attacks."[6] I agree with Lubell and I will use the term "cyber operations"

[1] *See What If People Were Paid for Their Data?: Advocates of "Data as Labour" Think Users Should be Paid for Using Online Services*, ECONOMIST (July 7, 2018), https://www.economist.com/the-world-if/2018/07/07/what-if-people-were-paid-for-their-data.

[2] Michael Riley, Sarah Frier & Stephanie Baker, *Understanding the Facebook-Cambridge Analytica Story: Quick Take*, WASHINGTON POST, Apr. 9, 2018, https://www.washingtonpost.com/business/understanding-the-facebook-cambridge-analytica-story-quick-take/2018/04/09/0f18d91c-3c1c-11e8-955b-7d2e19b79966_story.html.

[3] *What If People Were Paid for Their Data?*, *supra* note 1.

[4] A recent example of this tendency involved journalists reporting on the September 2018 cyber security breach at Facebook in which approximately 50 million users had their individual access tokens compromised. *See, e.g.*, Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES, Sept. 28, 2018, https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html; *see also* Julia Carrie Wong, *Facebook Says Nearly 50m Users Compromised in Huge Security Breach*, GUARDIAN (London) Sept. 29, 2018, https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach.

[5] Noam Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, 89 INTERNATIONAL LAW STUDIES 252, 258 (2013).

[6] *Id.*

throughout this article, unless citing another scholar or explicitly referring to an attack regulated by international humanitarian law.

It is important for present purposes to understand the meaning of "civilian objects" and "military objectives" and the implications of these meanings for electronic data. As Lubell suggests, in regulating the conduct of armed conflict, international humanitarian law uses "attack" as a term of art and specifies a number of limitations.[7] Additional Protocol I defines attack as "acts of violence against the adversary, whether in offence or in defence."[8] In turn, international humanitarian law prohibits parties from intentionally directing an attack against civilians or civilian property.[9] The basic rule on distinction, codified in Article 48(1) of Additional Protocol I, is that parties to an armed conflict must "distinguish between the civilian population and combatants and between civilian objects and military objectives."[10] This rule is integral to international humanitarian law and manifests in the twin prohibitions that: (1) "The civilian population as such, as well as individual civilians, shall not be the object of attack"[11] and (2) "Civilian objects shall not be the object of attack . . . ."[12] The rule also manifests in the concomitant directive that "[a]ttacks shall be limited strictly to military objectives."[13]

Article 52(1) of Additional Protocol I defines civilian objects as "all objects which are not military objectives" and Article 52(2) defines military objectives as "limited to those objects which by their nature location, purpose or use make an effective contribution to military action . . . ."[14] Both definitions—what a civilian object is not and what a military objective is—imply tangibility with their mutual emphasis on objects. This implied tangibility, of physical materiality, is made explicit in the International Committee of the Red Cross (ICRC) *Commentary on the Additional Protocols*.

> The English text uses the word "objects," which means "something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing." The

[7] *Id.*

[8] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 49(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

[9] *Id.* art. 48.

[10] *Id.*

[11] *Id.* art. 51(2).

[12] *Id.* art. 52(1).

[13] *Id.* art. 52(2).

[14] *See id.* art. 52(1)–(2).

> French text uses the word "biens," which means, "chose tangible, susceptible d'appropriation." It is clear that in both English and French the word means something that is visible and tangible.[15]

In drafting the *Tallinn Manual on the International Law Applicable to Cyber Warfare*,[16] (*Tallinn Manual 1.0*) the International Group of Experts had to grapple with the meaning of military objective and the implications of the definition for cyber operations. It is clear that the wording of Additional Protocol I and of the ICRC's *Commentary*, particularly to Article 52(2), influenced the drafting of *Tallinn Manual 1.0* on this point, and, in my view, those sources are entirely appropriate sources of influence. While the International Group of Experts unanimously agreed, "computers, computer networks and other tangible components of cyber infrastructure constitute objects,"[17] opinions in the group were divided on the characterization of data. The majority of experts were of the view that "an attack on data *per se* does not qualify as an attack" because the intangibility of data is neither consistent with the "ordinary meaning of the term object" nor "comports with the explanation of it in the ICRC Additional Protocols 1987 Commentary."[18] The majority of the International Group of Experts did agree that "a cyber operation targeting data may sometimes qualify as an attack when the operation affects the functionality of cyber infrastructure or results in other consequences that would qualify the cyber operation in question as an attack."[19]

While the majority of experts did not explain what they meant by those "other consequences," presumably the majority would include attacks against targets subject to special legal protection, such as hospitals, medical personnel and medical transport vehicles, vessels and aircraft, historic monuments, works of art, places of worship, as well as dams, dikes, nuclear electrical generating stations, and other works or installations containing forces dangerous to the civilian population.

[15] COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶¶ 2007–08 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

[16] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL 1.0].

[17] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, cmt. to r. 100, ¶ 5, at 437 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

[18] *Id.*

[19] *Id.*

A minority of experts took a different view of the "objectification" of some data. These experts held:

> [T]he majority position is under inclusive in the sense that failure to include cyber operations targeting data *per se* in the scope of the term "attack" would mean that even the deletion of essential civilian datasets such as social security data, tax records, and bank accounts would potentially escape the regulatory reach of the law of armed conflict, thereby running counter to the principle . . . that the civilian population enjoys general protection from the effects of hostilities. For these Experts, the key factor, based on the underlying object and purpose of Article 52 of Additional Protocol I, is one of severity and the operation's consequences, not the nature of harm. Thus, they were of the view that, at a minimum, civilian data that is "essential" to the well-being of the civilian population is encompassed in the notion of civilian objects and protected as such.[20]

The faithful recording of differences of opinion between the majority and the minority of the international group of experts is a recurrent and welcome feature of both *Tallinn Manuals*. My interest here is to identify and discuss the ramifications that flow from this particular difference of opinion. If data is an object, the rule on distinction applies and international humanitarian law prohibits the targeting of civilian data in the context of an armed conflict. If data does not constitute an object, the targeting of data *per se* is not unlawful and the rule on distinction does not apply.

Two common intuitive responses on the importance of civilian data support the minority view. One response favors maximum protection of the civilian population—consistent with a particular perspective on the motivation of international humanitarian law. The other response focuses on the contemporary ubiquity and increasing sensitivity to dependence upon data. I am not suggesting these two responses are exhaustive of reactions to the difference of opinion among the international group of experts, nor do I suggest that the two responses cannot coexist in the reactions of particular scholars. I merely observe that the responses are conceptually distinct. However, it is also true that both responses are often articulated over-simplistically as respective reactions to the majority view that data is not an object. That overly simplistic reactive tendency is the principal reason for my decision to characterize both response as "intuitive."

[20] *Id.* cmt. to r. 100, ¶ 6, at 437.

At different times in the past, I have had both responses, so I readily accept just how easy it is to entertain either position. For example, in a 2014 article co-authored with Rain Liivoja, we asked whether "the time has perhaps come to seriously consider whether an 'object' for the purposes of the targeting rules in LOAC necessarily needs to have corporeal existence."[21] *Tallinn Manual 1.0* was published in 2013 and the text finalized some time before that. In the intervening years, I have speculated whether, if the International Group of Experts for *Tallinn 1.0* reconvened to vote on whether an attack on data *per se* would constitute an attack, the original majority position would prevail, or whether some of the experts now would change their original position such that the minority now reflected that of a new majority.

Of course, others have noticed the lack of unanimity within the *Tallinn 1.0* group of experts on this issue. Heather Harrison Dinniss[22] and Kubo Mačák,[23] for example, both contributed to a symposium issue of the *Israel Law Review* in which they challenged the majority *Tallinn 1.0* position, albeit on different reasoning. Michael Schmitt commented on both of their papers,[24] defending the *Tallinn 1.0* majority view.

Schmitt, writing on his view of the *lex lata* in 2012, explicitly acknowledged that international law might rapidly evolve in response to the question of whether data constitutes an object, stating:

> I will slavishly adhere to the *lex lata*. I have set out elsewhere my views on where the law might be headed, but in this article, I merely comment on the state of the law as of July 2012. Although I believe the law on the notion of objects will evolve with some rapidity, speculation is not my purpose here. I do realise that the majority's interpretation of objects leads to undesirable results in the sense that it opens the door to cyber operations against data that could have a significant negative impact on the civilian population. However, an all-inclusive treatment of data as an object would,

[21] Rain Liivoja & Tim McCormack, *Law in the Virtual Battlespace: The* Tallinn Manual *and the* Jus in Bello, 15 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 45, 53 (2012).

[22] *See* Heather A. Harrison Dinniss*, The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 ISRAEL LAW REVIEW 39 (2015).

[23] *See* Kubo Mačák, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, 48 ISRAEL LAW REVIEW 55 (2015).

[24] Michael N. Schmitt, *The Nature of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision*, 48 ISRAEL LAW REVIEW 81 (2015).

> as will be explained, be over-inclusive. Until states determine the appropriate balance, it would be precipitate to extend the meaning of objects to this degree.[25]

The differing analysis and back-and-forth exchange between Harrison Dinniss, Mačák, and Schmitt is helpful in clarifying the parameters of the position articulated by the majority of experts. I will engage with that discussion before moving to supplementary analysis.

It is often wrongly assumed that the majority position leads inexorably to the view that any attack on data is permissible because data is not an object. That is not an accurate reflection of the majority position. Schmitt identifies a recurrent fallacy: "critics of the majority approach sometimes conflate the legal meaning of the term 'attack' as used in Rule 37 [now Rule 100] and that of 'object,' the issue at hand with regard to data."[26] The International Group of Experts unanimously agreed to the articulation of Rule 30 [now Rule 92], as they did to all the black letter rules, on the definition of a cyber attack: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[27] Accordingly, any operation undertaken against data with any of the aforementioned effects, the expected causing of injury or death to persons or damage or destruction of objects, would constitute an attack to which the rules on targeting apply. In the Commentary to Rule 92, the Group of Experts stated:

> The limitation in this Rule to operations against individuals or physical objects should not be understood as excluding cyber operations against data (which are non-physical entities) from the ambit of the term attack. Whenever an attack on data results in the injury or death of individuals or damage or destruction of physical objects, those individuals or objects constitute the "object of attack" and the operation therefore qualifies as an attack. Further, as discussed below, an operation against data upon which the functionality of physical objects relies can sometimes constitute an attack.[28]

Thus, operations undertaken against data with flow-on physically damaging effects are unquestionably attacks that are subject to international humanitarian law on distinction, proportionality, and precautions in attack.

[25] *Id.* at 84.

[26] *Id.* at 86.

[27] *See* TALLINN MANUAL 2.0, *supra* note 17, r. 92, at 415.

[28] *Id.* cmt. to r. 92, ¶ 6, at 416.

Here, there is no disagreement between the majority and the minority. All the *Tallinn 1.0* experts agree unanimously on the characterization of such operations as attacks.

Beyond those operations against data, which result in physically damaging effects, hypothetical examples help to clarify the parameters of the majority position. Mačák, for example, offered two examples to challenge the majority position. Both examples were intended to illustrate cyber operations designed to destroy data without physical force that States would likely consider as constituting "attacks" because of the non-physical, but nevertheless significant, consequences of the operations. Schmitt's view is that neither example achieves its intended purpose. Both the examples and Schmitt's counter-analysis are helpful.

First, Mačák raises the example of targeting "critical data of a military nature, such as weapons logs, timetables for the deployment of military logistics, or air traffic control information."[29] In each case, he argues that the data itself is a legitimate military objective because it "makes an effective contribution to the military action of one party . . . [and] its destruction would, therefore, also offer a definite military advantage to the opposing party."[30] Mačák asserts that States would probably accept that such data constitutes a legitimate military objective.[31]

Schmitt's response is instructive. The critical question is whether data is an object. If it is, then in all three cases the data is a military objective and can be attacked. If data is not an object, as Schmitt asserts, "it may still be 'targeted' because the prohibition on attacking civilian objects does not attach."[32] The result is the same either way, as parties can legitimately target and destroy the date, and, in Schmitt's view, "States would be comfortable with either approach."[33]

Harrison Dinniss approaches her critique of the majority position differently, but one of her key examples is similar to Mačák's first example. While other commentators show concern that the rejection of data as an object fails to protect civilian data, Harrison Dinniss instead notes that the rejection of data as an object may lead to immunity from attack for military data:

[29] Mačák, *supra* note 23, at 76.

[30] *Id.*

[31] *Id.*

[32] Schmitt, *supra* note 24, at 98.

[33] *Id.*

> To take a practical example, weapons, weapons systems and military *matériel* are perhaps the epitome of a legitimate military objective. Malware that is designed specifically to cause death, injury, destruction or damage is indisputably a weapon. Examples include Stuxnet-type code, which is intended to cause physical destruction, or even viruses such as Wiper, which destroyed the functionality of computer systems without destroying any physical components. However, by excluding intangible objects such as code from the interpretation of the definition offered by the majority of the Tallinn group, neither of these cyber weapons would constitute a legitimate military objective. It cannot be correct that one can have a weapon that is made entirely from code that does not constitute a military objective.
>
> As the definition of civilian objects is provided in a negative form – that is, civilian objects are all things that are not military objectives – we are left with two main alternatives. Either a piece of code such as Stuxnet is a civilian object or, given that the problem is with the term "object" itself, it is not covered by the definition of military objectives at all. Given that the object and purpose of both the principle of distinction and of the Additional Protocol itself is to provide effective protection for civilians and civilian objects while enabling parties to an armed conflict to conduct effective military operations, either of those alternatives produces a manifestly unreasonable result. In order to conduct efficient military operations against cyber targets while minimising the harm to civilians and civilian objects, it will sometimes be necessary to conduct attacks against code rather than the physical infrastructure on which it rests. Any modern interpretation of the law should reflect this necessity and allow for that to happen.[34]

Schmitt dismisses the concern as he did Mačák's first example, noting "[i]rrespective of the view one takes on the object issue, Stuxnet-like code is clearly targetable in an armed conflict."[35] If data is not an object, as the *Tallinn 1.0* majority asserts, then the prohibition on targeting civilian objects does not apply and Stuxnet-like code is targetable. However, even if data is an object, the *Tallinn 1.0* minority position, Stuxnet-like code unquestionably satisfies the Additional Protocol I Article 52(2) criteria for a legitimate military objective.[36]

This is an important clarification on the scope of the *Tallinn 1.0* majority's position. It is fallacious to assume that if data is not considered an object, militaries will be restricted in their freedom to target and destroy data

[34] Harrison Dinniss, *supra* note 22, at 44–45.

[35] Schmitt, *supra* note 24, at 103.

[36] Additional Protocol I, *supra* note 8, art. 52(2).

that is being used by an adversary for military purposes. That assumption is simply a misunderstanding of the implications flowing from the majority's position. I do not mean to imply here that these examples from Mačák and Harrison Dinniss are unhelpful. In fact, Harrison Dinniss is entirely accurate when she states, "In order to conduct efficient military operations against cyber targets while minimising the harm to civilians and civilian objects, it will sometimes be necessary to conduct attacks against code rather than the physical infrastructure on which it rests."[37]

The limitation with the majority position is not that military code cannot be targeted. Rather, it is that civilian code can also be targeted. Because the majority does not consider code an object, the law of targeting does not apply to operations directed against it. The examples provided by Mačák and Harrison Dinniss, as well as Schmitt's explanatory responses, all illustrate how readily the *Tallinn 1.0* majority position evokes intuitive reactions sometimes based on erroneous assumptions. Even Schmitt concedes, in relation to the majority's discussion of the question of tangibility versus intangibility for targetable military objectives, that "in fairness to both of them [Mačák and Harrison Dinniss] a more robust discussion of the issue might have added clarity."[38]

Mačák's second example involves the targeting of essentially civilian data, "such as electric health records held at a particular hospital."[39] He notes:

> If this data were to be clandestinely erased or altered, the lives and health of patients in the hospital would be endangered. This data does not, of course, meet the criteria of a military objective; its destruction would rather affect the integrity of a civilian object (the data itself) and the safety of the civilian population (the patients in the hospital). . . . Both of these examples share the fact that the direct consequence of the attacks considered would be solely the destruction of data. For the Tallinn Manual [1.0], such attacks would normally fall outside the scope of IHL unless, in addition, they were to interfere with the functionality of the control system to an extent requiring the replacement of physical components.[40]

Schmitt's response is that any such targeting of electronic health records at a hospital would not fall outside the scope of international humanitarian law.

[37] Harrison Dinniss, *supra* note 22, at 45.

[38] Schmitt, *supra* note 24, at 103.

[39] Mačák, *supra* note 23, at 76.

[40] *Id.* at 76–77.

> To begin with, the operation is an attack irrespective of the targeting of the data because of the potential foreseeable harm to patients. As the IGE [International Group of Experts] noted without dissent, the requisite consequences to qualify as an attack "include any foreseeable consequential damage, destruction, injury or death" and, accordingly, "[w]henever an attack on data results in the injury or death of individuals . . . those individuals . . . constitute the 'object of attack' and the operation qualifies as an attack." Further, foreseeable collateral damage of the qualifying nature would also render the operation in question an attack. Finally, the example is inapposite because the IGE unanimously concluded in Rule 71 [now Rule 131] that "data that form an integral part of the operations or administration of medical units and transports must be respected and protected, and in particular may not be made the object of attack."[41]

The point of Mačák's two examples is to expose the limitations of the *Tallinn 1.0* majority's position that data is not an object. Schmitt's responses to both examples demonstrate that the implications of the majority position are slightly more nuanced than intuition might suggest. Data that might otherwise constitute a legitimate military objective can lawfully be targeted and destroyed whether or not data is an object. Civilian health records cannot lawfully be targeted and destroyed whether or not data is an object. The real point of contention is the characterization of cyber operations directed against civilian data where no physical damage occurs or is reasonably expected to occur.

Perhaps the sort of examples Mačák and others wanting to support the *Tallinn 1.0* minority position need to provide are those that involve cyber operations directed against civilian data that result in the destruction or deletion of the data with no additional physical consequences. If data qualifies as an object, such operations directed against civilian data would constitute unlawful attacks. The *Tallinn 1.0* minority briefly raise some possibilities, which they offer as the basis for their disagreement with the majority position.[42] Those possibilities are included in paragraph seven of the Commentary to Rule 100 of *Tallinn Manual 2.0*.[43] The minority considered that the exclusion of the targeting of data *per se* from the scope of an "attack" would mean

[41] Schmitt, *supra* note 24, at 98.

[42] TALLINN MANUAL 1.0, *supra* note 16, cmt. to r. 38, ¶ 5, at 127.

[43] TALLINN MANUAL 2.0, *supra* note 17, cmt. to r. 100, ¶ 7, at 437.

> even the deletion of essential civilian datasets such as social security data, tax records, and bank accounts would potentially escape the regulatory reach of the law of armed conflict, thereby running counter to the principle . . . that the civilian population enjoys general protection from the effects of hostilities.[44]

These are helpful examples and I will return to them in due course. For now, it is important to note that Schmitt concedes the normative truth of the minority's position if his, and the majority's view, is incorrect.[45]

III. THE INCREASING SIGNIFICANCE OF DATA AND THE DELETERIOUS IMPACT OF CYBER OPERATIONS

It would be difficult to remain unaware of the growing sensitivities to the significance of data and of the outrage at the increased sophistication of cyber operations directed against it. The following relatively recent experiences are indicative of these trends and perhaps help to explain intuitive reactions to the *Tallinn 1.0* majority position. I offer the following examples to illustrate the trends that I am describing. Later, I will return to the question of whether, if any of these examples had occurred in the context of an armed conflict, they would have constituted an attack subject to the rules of international humanitarian law if data does indeed constitute an object.

Security breaches resulting in the exfiltration of data are commonplace.[46] One particularly high-profile incident involved the unauthorized penetration of the databases of the U.S. Office of Personnel Management (OPM) in 2015, which resulted in the alleged exfiltration of personal information of

[44] *See* TALLINN MANUAL 2.0, *supra* note 17, cmt. to r. 92, ¶ 6, at 416.

[45] Schmitt, *supra* note 24, at 97.

> Since data is not an object, then on that basis it is not subject to the prohibition on attacking civilian objects; it is instead necessary to look to the consequences of its damage or destruction to determine whether the prohibition applies. However, as I have just noted above, I concede that if data is an object as a matter of law, the prohibition applies, albeit only if the cyber operation in question qualifies as an attack because the data has been damaged or destroyed.

[46] According to Techopedia, data exfiltration is "the unauthorized copying, transfer or retrieval of data from a computer or server. Data exfiltration is a malicious activity performed through various different techniques, typically by cybercriminals over the Internet or other network. Data exfiltration is also known as data extrusion, data exportation or data theft." *See* TECHOPEDIA, TECHNOLOGY DICTIONARY: EXFILTRATION, https://www.techopedia.com/definition/14682/data-exfiltration (last visited Oct. 23, 2018).

more than 22 million U.S. government employees.[47] It is not alleged that any of this data was lost or destroyed. The issue was that this vast amount of highly sensitive personal data was unlawfully copied and that the data allegedly included not only details such as full name, date of birth, home address, credit card details, social security numbers, tax file numbers, passport numbers, and digital fingerprint records—a level of detail that could clearly facilitate identity theft—but also entire files for national security clearance processes to authorize access to highly sensitive U.S. government information. Anyone who has been subjected to national security screening processes in his or her own country will appreciate just how intrusive the questioning, and subsequent disclosure of personal information, is.

I have written elsewhere about the OPM hack, particularly the hyperbole in the ensuing public debate about the significance of the access to and theft of that information.[48] I was surprised to read characterizations of this incident as "an act of war" or "cyber Pearl Harbor," or that some commentators considered it even more serious than the 9/11 attacks because of the potential threat to U.S. national security that the targeted theft of sensitive personal information from such a large number of senior public servants constituted.[49] There is no suggestion that the Obama administration characterized the operation in these terms. On the contrary, the administration received considerable criticism for not characterizing the operation in more severe terms,[50] even though, from the perspective of international humanitarian law, it was correct not to do so. But an accurate legal analysis of what happened ought not to obfuscate the seriousness of the exfiltration of all that

[47] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASHINGTON POST, July 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

[48] *See* Tim McCormack, *The Sony and OPM Double Whammy: International Law and Cyber Attacks*, 18 SOUTHERN METHODIST UNIVERSITY SCIENCE AND TECHNOLOGY LAW REVIEW 379, 379–83 (2015) (comparing the OPM hack with the Sony Corporation hack). The Sony hack not only involved the loss of massive quantities of company data including details of yet-to-be released movies, it also resulted in a loss of functionality of at least 2,500 computers. The OPM hack, in contrast, involved only the exfiltration of the data in question and no loss of functionality or destruction of any hardware. *See id.*

[49] *Id.* at 381–82.

[50] *See, e.g.*, Kate Sheppard, *McCain Calls Sony Hack an 'Act of War,'* HUFFINGTON POST (Dec. 21, 2014), http://www.huffingtonpost.com/2014/12/21/sonynorth-korea-war n_6362454.html; Mike Levine, *OPM Hack: Top Lawmaker Says US 'Under Attack,'* ABC NEWS (June 16, 2015), https://abcnews.go.com/Politics/opm-hack-top-lawmaker-us-attack/story?id=31797366.

sensitive personal data, and the overwhelming majority of the millions of public servants directly affected were understandably annoyed that the breach had occurred.

Exfiltration of data, while all too commonplace, is not the end of the "sensitivities to operations directed at data" story. Indeed, the key cybersecurity event in 2017 was the repeated deployment of "ransomware." Here, WannaCry and NewPetra are perhaps the most well-known and devastating examples. Rather than the planting of malware to exfiltrate data, ransomware typically involves the deployment of malware to encrypt data rendering it inaccessible to its users. The malware then demands payment (usually in a cryptocurrency) for the decryption of the data, hence the "ransomware" descriptor. The WannaCry operation gained higher public profile in Australia because some business corporations were affected and media outlets reported extensively on the scale and speed that the malware spread. Early estimates suggested that more than 200,000 computers in 150 countries were impacted by the malware,[51] although later reports suggested the number of affected computers could have been as many as 300,000.[52]

Despite the scale and spread of the WannaCry malware, data was re-accessible on most of the affected computers within a few days because of the rapid development and subsequent availability of software patches to decrypt the data. It is not hard to imagine a global, collective sigh of relief that this operation, and others like it, were not more damaging in their effects. One key reason for the relatively small amount of permanent damage was that cybersecurity measures surrounding critical infrastructure in several countries was sufficiently current and robust to prevent the malware's crippling encryption. Here, I do not mean to imply that National Health Service hospitals in the United Kingdom, where data encrypted by the malware was rendered inaccessible for days, do not constitute critical infrastructure. The point I am trying to make is that despite the global reach of the malware, the damage was not as severe as it might have otherwise have been. That fact, however, does not obviate the reality that the virulence of WannaCry and

[51] *See, e.g.*, Henry Belot & Stephanie Borys, *Ransomware Attack Still Looms in Australia as Government Warns that WannaCry Threat Not Over*, ABC NEWS (May 16, 2017), http://www.abc.net.au/news/2017-05-15/ransomware-attack-to-hit-victims-in-australia-government-says/8526346.

[52] *See, e.g.*, Dustin Voltz, *U.S. Blames North Korea for 'WannaCry' Cyber Attack*, REUTERS (Dec. 19, 2017), https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q.

other ransomware contributed to a growing sensitivity to the importance of data to daily life in most of the world.

Governments hardly need convincing of the growing significance of data and the vulnerability of their respective societies to exponential increases in the number of cyber operations launched every year, or in the increased sophistication and capacity of these operations to do harm. It is reasonable to expect that growing sensitivity to the importance of data would translate into practical measures by States, unilaterally and collectively, to reflect their increasing concerns and that any such measures might extend to clarifying or developing international legal norms to regulate operations directed against data. But the issue here is not increasing awareness of the significance of personal data. The question is whether States are bound by a legal norm to the effect that data is an object thereby making the targeting of data subject to the rules of targeting during an armed conflict.

IV. Is Data an Object for the Purposes of the Application of International Humanitarian Law?

The position of the ICRC in 2015 was:

> There is also increasing concern about safeguarding essential civilian data. With regard to data belonging to certain categories of objects that enjoy specific protection under IHL, the protective rules are comprehensive. For example, the obligation to respect and protect medical facilities must be understood as extending to medical data belonging to those facilities. However, it would be important to clarify the extent to which civilian data that does not benefit from such specific protection, such as social security data, tax records, bank accounts, companies' client files or election lists or records, is already protected by the existing general rules on the conduct of hostilities. Deleting or tampering with such 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. The conclusion that this type of operation would not be prohibited by IHL in today's ever more cyber-reliant world – either because deleting or tampering with such data would not constitute an attack in the sense of IHL or because such data would not be seen as an object that would bring into operation the prohibition of attacks on civilian objects – seems difficult to reconcile with the object and purpose of this body of norms.[53]

[53] *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Document Prepared by the International Committee of the Red Cross for the 32nd International Conference of*

The difference of opinion between this articulation of the ICRC position and the *Tallinn 1.0* majority is not a vast chasm. As we have seen in relation to Mačák's second example discussed above, the majority position accepts the view of the ICRC quoted above that "data belonging to certain categories of objects . . . enjoy specific protection under IHL," and that this data retains that protection from attack.[54]

The ICRC is understandably concerned about civilian data that does not benefit from such specific protection, such as social security data, tax records, bank accounts, companies' client files, or election lists and records. The ICRC is keen to clarify "the extent to which such data is already protected by the existing general rules on the conduct of hostilities" and rightly highlights the possibility that "[d]eleting or tampering with such 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."[55] But the *Tallinn 1.0* majority also acknowledged that targeting data could result in certain debilitating physical consequences. So, for all *Tallinn* experts, the targeting of any such data resulting in death or serious harm, or causing physical damage extending to loss of functionality of computers or other physical cyber infrastructure would constitute an attack to which the rules of targeting apply.[56] The difference between the ICRC and the *Tallinn 1.0* majority is the same as that between the *Tallinn 1.0* majority and minority: whether operations directed at civilian data without deleterious physical consequences should also be subjected to the rules of targeting.

In relation to the examples above concerning the exfiltration of data from the OPM and the encryption of data by WannaCry ransomware, it is worth considering whether either act would constitute an attack assuming that both operations occurred during an armed conflict and that data is considered an object when applying international humanitarian law.

Assuming the OPM hack only involved the exfiltration of data with no loss or destruction of any of that data and no loss of functionality to the servers on which the data was stored, unauthorized exfiltration is akin to remote cyber espionage, that is, cyber espionage conducted outside of the

the Red Cross and Red Crescent, Geneva, 8–10 December 2015, 97 INTERNATIONAL REVIEW OF THE RED CROSS 1427, 1478 (2016).

[54] *Id.*

[55] *Id.*

[56] *See* TALLINN MANUAL 1.0, *supra* note 16, cmt. to r. 30, ¶ 6, at 107–08; TALLINN MANUAL 2.0, *supra* note 17, r. 92, at 415 and cmt. to r. 92, ¶¶ 2–6, at 415–16.

physical territory of the United States. It is widely accepted that cyber espionage in the context of armed conflict or in peacetime is not illegal *per se*.[57] Even if data is considered an object, exfiltration alone does not constitute an "attack" under the law of targeting. If, however, in the course of the penetration of the servers and the exfiltration of the data, some of the targeted data was corrupted or deleted, then, if data is an object, the operation may have constituted an attack subject to the law of targeting. Assuming that all the data was of a civilian nature, which probably cannot be assumed about the actual OPM hack given allegations of personal data for national security clearance purposes, the attack would have violated international humanitarian law. If WannaCry or similar ransomware had been launched in the context of an armed conflict and resulted in no more damage than temporary encryption of civilian data that was subsequently decrypted without loss of the data, again, this act would not constitute an "attack" under the law of targeting. If, however, in the course of malicious encryption of civilian data, some of that data was corrupted or deleted, then the operation would have constituted an attack and that attack would have violated international humanitarian law.

V. CONCLUSION

At present, we lack examples from armed conflict of cyber operations targeted against civilian data without deleterious physical consequences and, consequently, we also lack precedents for how States respond to the legal characterization of such incidents. The lack of relevant State practice renders how States might respond a speculative enterprise. There is undoubtedly a growing "objectification" of data as the incidence and sophistication of cyber operations dramatically increase. Ultimately, it will be for States to determine whether data is an object for the purposes of the law of targeting in the context of an armed conflict. In this period of uncertainty, Schmitt is right to observe that States may well consider it in their best interest not to clarify the precise legal position because there may well be "situations in which a State *would* want to target civilian data directly and therefore would hesitate to embrace an interpretive approach that would render it a civilian object."[58]

Perhaps the clarification will come in response to a future situation where one party to an armed conflict deliberately targets and destroys civilian

[57] *Id.* r. 32, at 168; r. 89, at 409.

[58] Schmitt, *supra* note 24 at 99 (emphasis in original).

banking records causing widespread anxiety but without causing any consequent physical damage, and the attacking State claims to have done so legitimately because data is not an object, thus rendering the rules on targeting inapplicable. If multiple States criticized that approach, not wanting the banking data of their own civilian population to be targeted in a future armed conflict, we may then have the clarification that many desire.

In 2018, I would support what was the minority position in 2011. When thinking about this issue, I fondly recall a familiar image from Tallinn, and it is not group singing at a local restaurant to the chagrin of all Estonians at our table, although that is certainly one image indelibly etched in my memory. I am in the room with the International Group of Experts and Michael Schmitt asks us to indicate our views as to whether data constitutes an object. It is not 2011, although I am not sure how I would have voted then. It is 2018, and I raise my hand in support of what was the minority position. I do so on the basis that the object and purpose of international humanitarian law is to protect the civilian population from the deleterious consequences of armed conflict. Part of my motivation in so voting would be a vested personal interest in not wanting my tax records, social security information, banking details, or other personal information the subject of targeted cyber operations if Australia becomes a party to an armed conflict in the future. But the international humanitarian lawyer in me would assert that personal vested interest is no basis for determining the existence of a binding legal norm. And if I was completely honest with myself, I suspect that there would be a quiet voice deep in the recesses of my mind asking plaintively but insistently – are you sure Timbo?