The Digital Geneva Convention

A Critical Appraisal of Microsoft's Proposal

Valentin Jeutner

Associate Senior Lecturer, Department of Law, Lund University, Sweden

valentin.jeutner@jur.lu.se

Abstract

Microsoft's 2017 call for a Digital Geneva Convention is a welcome contribution to the debate on how the global technology sector and the international civil society should respond to increased State-led cyberattacks. However, Microsoft's portrayal of cyberspace as a space devoid of regulation is inaccurate, especially in light of the rules contained in the *Tallinn Manual 2.0*. Microsoft's call for the establishment of an international attribution organization overlooks existing international legal mechanisms. The characterization of global technology firms as 'first responders' providing services akin to those provided by the Red Cross societies is imperfect since technology companies are, compared to the Red Cross, non-neutral and profit-making enterprises.

Keywords

Geneva Conventions – international humanitarian law – global technology sector – Tallinn Manual – Microsoft – Red Cross

One day in June 1859, a young Henri Dunant came across the battlefield of Solferino. He witnessed how the French and Sardinian forces fought the army of the Austrian Empire 'with the impetuosity of a destructive torrent that carries everything before it'.¹ At the end of the day, as the battle concluded, '[men] of all nations lay side by side on the flagstone floors of the churches of Castiglione ... Oaths, curses and cries such as no words can describe resounded from

1 Henry Dunant, *A Memory of Solferino* (International Committee of the Red Cross 1959) 18.

the vaulting of the sacred buildings.² What concerned Dunant most was that wounded men ‘who could have been saved’³ were left to die on the battlefield. Thus, Dunant resolved to set up ‘relief societies for the purpose of having care given to the wounded in wartime’.⁴ Subsequently, Dunant’s efforts led to the adoption of the 1864 Geneva Convention⁵ and to the foundation of an organization that would become known as the International Committee of the Red Cross (‘ICRC’) in February 1863.

In February 2017, Microsoft’s President, Brad Smith, invoked the legacy of the ICRC in support of a proposal to address contemporary cybersecurity challenges.⁶ According to Smith, the ‘world of potential war has migrated from land to sea to air and now cyberspace’.⁷ Consequently, the global technology sector faces the problem that ‘74 percent of the world’s businesses expect to be hacked’ and that the ‘economic loss of cybercrime is estimated to reach \$3 trillion by 2020’.⁸ Smith adds that these problems are exacerbated by an increase in ‘cyberattacks’ carried out by States.⁹ As five examples of such ‘attacks’¹⁰ he lists the attack on Iran’s nuclear infrastructure,¹¹ the alleged Chinese hacking

2 Ibid 61.

3 Ibid 19.

4 Ibid 115.

5 Convention for the Amelioration of the Condition of the Wounded in Armies in the Field (1884) (adopted 22 August 1864, entry into force 22 June 1865, not in force since 16 August 1966).

6 A video of Smith’s presentation is available here: RSA Conference, *Protecting and Defending against Cyberthreats in Uncertain Times* <www.youtube.com/watch?v=kP_yf_Uz4vc> accessed 4 January 2019. A transcript of the presentation is available here: Brad Smith, ‘Transcript of Keynote Address at the RSA Conference 2017: “The Need for a Digital Geneva Convention”’ (San Francisco, 14 February 2017) 3 <news.microsoft.com/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf> accessed 4 January 2018.

7 Smith (n 6) 3.

8 Brad Smith, ‘The Need for a Digital Geneva Convention’ (*Microsoft on the Issues*, 14 February 2017) para 4 <blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention> accessed 19 February 2017.

9 Smith (n 6) 1.

10 The use of the term ‘attack’ here is not meant to imply that the mentioned incidents were attacks in an international legal sense.

11 Mark Clayton, ‘How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant’ *Christian Science Monitor* (16 November 2010) <www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant> accessed 8 January 2019.

of US companies,¹² the takedown of Ukraine's power grid,¹³ the North Korean attack on Sony Pictures,¹⁴ and the attack of the US Democratic National Committee in the run-up to the 2016 US presidential elections.¹⁵ Smith proposes a trilogy of measures to address the identified problems.

First, States should adopt a Digital Geneva Convention. Modelled on international humanitarian law's Four Geneva Conventions, Smith argued States should 'create a legally binding framework to govern states' behaviour in cyberspace'.¹⁶

Secondly, Microsoft argues that a 'new independent organization, a bit like the International Atomic Energy Agency' ('IAEA') should be created. Such an organization should be tasked with identifying 'attackers when nation-state attacks happen'.¹⁷ It would be a 'private sector-led, independent and transparent [organization]...with a singular focus on' attributing 'state or state-sponsored cyberattacks'.¹⁸

Thirdly, as the 'world's first responders'¹⁹ to cyberattacks, global technology companies should come together like 'the ICRC did in 1949' and 'sign [its] own pledge in conjunction with the world's states'.²⁰ Such a pledge should contain

- 12 Pierre Thomas and Mike Levine, 'US Charges 5 Chinese Military Hackers in "21st Century Burglary"' *ABC News* (19 May 2014) <abcnews.go.com/US/us-charges-chinese-military-hackers-21st-century-burglary/story?id=23774172> accessed 8 January 2019.
- 13 Jordan Robertson and Michael Riley, 'How Hackers Took Down a Power Grid' *Bloomberg* (14 January 2016) <www.bloomberg.com/news/articles/2016-01-14/how-hackers-took-down-a-power-grid> accessed 8 January 2019.
- 14 Ellen Nakashima, Craig Timberg and Andrea Peterson, 'Sony Pictures Hack Appears to Be Linked to North Korea, Investigators Say' *Washington Post* (3 December 2014) <www.washingtonpost.com/world/national-security/hack-at-sony-pictures-appears-linked-to-north-korea/2014/12/03/6c3c7e3e-7b25-11e4-b821-503cc7efed9e_story.html> accessed 8 January 2019.
- 15 Katiana Krawchenko and others, 'The John Podesta Emails Released by WikiLeaks' *CBS News* (3 November 2016) <www.cbsnews.com/news/the-john-podesta-emails-released-by-wikileaks> accessed 8 January 2019.
- 16 Microsoft, 'A Digital Geneva Convention to Protect Cyberspace', *Microsoft Policy Papers* 1 <www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace> accessed 3 January 2019.
- 17 Smith (n 6) 11.
- 18 Microsoft, 'An Attribution Organization to Strengthen Trust Online', *Microsoft Policy Papers* 2 <query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67Q1> accessed 7 January 2019.
- 19 Smith (n 6) 4.
- 20 Ibid 12.

two key commitments: to ‘assist and protect customers everywhere’ and not to ‘aid in attacking customers anywhere.’²¹

Microsoft’s proposals received widespread attention and support. For example, in the run-up to the German Federal Election 2017 Deutsche Telekom, Europe’s largest telecommunications provider, joined the call for a Digital Geneva Convention²² and more than 60 companies have signed Microsoft’s Cybersecurity Tech Accord²³ which is designed to facilitate the realization of the third part of Smith’s 2017 proposal.

Despite, or rather because of, the support that Microsoft’s proposal received, this contribution scrutinizes each of Microsoft’s three proposals. With respect to the first proposal, it is concerning to portray cyberspace as non-norm governed territory. With respect to the proposed attribution organization it is problematic to assume that technical competence equates to legal competence. Finally, it will be argued that equating the services provided by the Red Cross to those of technology service providers is an imperfect analogy. It will be noted, however, that the technology sector’s commitment to be mindful of the political nature of their conduct and of the context within which they operate is welcome.

1 Cyberspace is Not Non-norm-governed Territory

Smith described cyberspace as a new battlefield that ‘the world has [not] seen before.’²⁴ The description of cyberspace as a new territory assumes that a ‘legal void exists regarding cyber-attacks’,²⁵ that cyberspace is ‘an unregulated or quasi-regulated space.’²⁶ The characterization of cyberspace as *terra nullius* or even as a space that ‘cannot be found in the physical world’²⁷ is significant. It is

21 Ibid 13.

22 Deutsche Telekom AG, ‘Stopping the Downward Spiral’ (28 June 2017) <www.telekom.com/en/company/details/stopping-the-downward-spiral-497812> accessed 4 January 2019.

23 ‘Cybersecurity Tech Accord’ <cybertechaccord.org> accessed 8 January 2019.

24 Smith (n 6) 3.

25 David Wallace and Mark Visger, ‘Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology’ (2018) 6 Journal of Law and Cyber Warfare 3, 16.

26 Robers Gorwa and Anton Peez, ‘Tech Companies as Cybersecurity Norm Entrepreneurs: A Critical Analysis of Microsoft’s Cybersecurity Tech Accord’ 10 <doi.org/10.31235/osf.io/g56c9> accessed 6 January 2019.

27 Smith (n 6) 3.

an invitation to call for the creation of new norms. But it is also a narrative that calls into question the validity of established norms. It creates the impression that there exists a legal leeway. This can lead to progressive developments of law. But it can also lead to departures from longstanding legal principles. There is a difference between the position that existing law applies to cyberspace, the position that existing law should be applied to cyberspace, the position that law currently applied to cyberspace needs to be improved and the position that altogether new norms are needed to govern cyberspace. When calling for a Digital Geneva Convention, Microsoft takes the last position. However, Microsoft's characterization of cyberspace as *terra nullius* is misleading and overstates²⁸ the need for novel regulation.

While it is correct that '[i]nteractions and communities formed in [cyberspace] are often deterritorialized',²⁹ cyberattacks conducted by States are, in principle and like any other State conduct, governed by international law.³⁰ Naturally, States and corporations reluctant to submit their cyber operations to legal scrutiny might have an interest in arguing that cyberspace is unlike anything international law has seen before. However, the International Court of Justice ('ICJ') has explicitly clarified that both the law of war and the law of armed conflict are applicable to cyberspace. With respect to the international law governing times of war, the ICJ held that the *ius ad bellum*, the prohibition of the use of force and the corresponding exceptions (essentially articles 2(4), 42, 51 of the UN Charter³¹), apply to 'any use of force, regardless of the weapons employed'.³² With reference to the *ius in bello* (the laws governing the conduct of armed conflict) the Court confirmed that 'the established principles and rules of humanitarian law applicable in armed conflict' apply 'to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future'.³³ The *Tallinn Manual 2.0* echoes these

28 Wallace and Visger (n 25) 9–10.

29 Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 *American Journal of International Law* 583, 653.

30 And, of course, by applicable domestic laws and norms of regional or subject-specific organizations.

31 Charter of the United Nations (1945) 1 UNTS XVI.

32 *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* [1996] ICJ Rep 226 [39]. See also Michael N Schmitt and International Group of Experts convened by the NATO Cooperative Cyber Defence Centre of Excellence (eds), *Tallinn Manual 2.0* (Cambridge University Press 2017) 330 (rule 69); Wallace and Visger (n 25) 27.

33 *Nuclear Weapons* (n 32) [86]. See also, Cordula Droegel, 'Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 *International Review of the Red Cross* 533, 578.

statements. It observes that '[d]espite the novelty of cyber operations ... the law of armed conflict applies to such activities during both international and non-international armed conflicts.'³⁴ The *Tallinn Manual 2.0* is not an official legal document and has been received cautiously by some States.³⁵ However, it does constitute a comprehensive and peer-reviewed 'objective restatement'³⁶ of the existing law that was informed by the unofficial comments of over 50 States.³⁷

Since Smith referred specifically to the challenge of regulating cyberattacks at times of peace,³⁸ it should be noted that, compared to its first edition, the *Tallinn Manual 2.0* now explicitly considers 'key aspects of the public international law governing "cyber operations" during peacetime'.³⁹ Eleven of the *Tallinn Manual 2.0*'s twenty chapters deal with law applicable at times of peace. The manual's authors distilled existing international law on cybersecurity into 64 rules covering *inter alia* international human rights law, diplomatic immunity law, space law or international telecommunications law. With respect to the incidents that Smith mentioned, it has been shown⁴⁰ that they are covered by international law. If one assumes, for the sake of argument (as Smith appears to assume), that the mentioned incidents are cyberattacks carried out by States, all (with the exception of the Chinese hacking of US companies) would at the least violate the international norms expressed by Rule 4 of the *Tallinn Manual 2.0*: 'A State must not conduct cyber operations that violate the sovereignty of another State.' The principle of sovereignty in this context extends to both government and private cyber infrastructure.⁴¹

To the extent that the takedown of Ukraine's power grid and the interference with the Iranian nuclear infrastructure resulted in physical consequences on their territories, the cyberattacks would also engage the manual's Rule 66 (prohibited intervention), Rule 68 (unlawful use of force), and Rule 71 (armed attack). Rule 66 concerning the prohibition to intervene 'in the internal or external affairs of another State' by cyber means would also apply to the hacking of the Democratic National Committee since the related interference in the US election could be seen to undermine the ability of the US to 'independently

34 *Tallinn Manual 2.0* (n 32) 375 (rule 80 (para 1)).

35 See generally, Efrony and Shany (n 29).

36 *Tallinn Manual 2.0* (n 32) 3.

37 Ibid 6.

38 Smith (n 6) 9.

39 *Tallinn Manual 2.0* (n 32) 3.

40 Wallace and Visger (n 25) 30–35.

41 *Tallinn Manual 2.0* (n 32) 18.

decide on its political, social, cultural, economic, and legal order.⁴² With respect to the alleged Chinese hack of US companies, the authors of the *Tallinn Manual 2.0* are admittedly 'divided over the unique case of cyber espionage'.⁴³ They observe that 'customary international law does not prohibit espionage *per se*'.⁴⁴ The legal ambivalence concerning espionage is, however, not unique to cyberspace, but rather a general feature of international law.⁴⁵

Overall, therefore, it is misleading to characterize cyberspace as a space devoid of regulation. Certainly, existing norms are being violated and one needs to think carefully about how norms crafted for the analogue realm can be applied to cyberspace. However, both of these aspects are ordinary features of the legal process⁴⁶ and not indicative of a lack of regulation. The call for new legal norms by powerful stakeholders like Microsoft, compared to arguments in favour of the application or extension of existing norms to cyberspace, can under these circumstances create uncertainty and can have destabilizing effects. It would be more productive to focus on improving the enforcement of existing norms. The next section will consider to what extent Microsoft's proposal to establish a new attribution organization could serve that aim.

2 Technical Expertise Does Not Equate to Legal Competence

Microsoft's second suggestion is to establish an 'attribution organization' that could 'receive and analyze ... evidence related to a suspected state-backed cyberattack, and that could then credibly and publicly identify perpetrators'.⁴⁷ The basis of such an organization should be the 'expertise of private sector technology firms'⁴⁸ and any findings would be peer-reviewed.⁴⁹ The organization

42 Ibid 15.

43 Ibid 19.

44 Ibid 169.

45 See, eg, Stefan Talmon, 'Tapping the German Chancellor's Cell Phone and Public International Law – Cambridge International Law Journal' (*Cambridge International Law Journal Online*, 6 November 2013) <cilj.co.uk/2013/11/06/tapping-german-chancellors-cell-phone-public-international-law> accessed 8 January 2019.

46 Indeed, Finnemore and Hollis observe: 'Norms elsewhere have had to deal with rapidly changing situations and technologies, with a similar global scope and scale'. See Martha Finnemore and Duncan B Hollis, 'Constructing Norms for Global Cybersecurity' (2016) 110 *American Journal of International Law* 425, 478.

47 Microsoft (n 18) 1.

48 Ibid.

49 Ibid 2.

would be designed to address the problem that ‘there is no organization that can present a politically-neutral and fact-based analysis ... when states allege that geopolitical rivals have targeted them’.⁵⁰

The rationale of Microsoft’s proposal to establish an independent ‘watch-dog’⁵¹ organization appears to be informed by the assumption that there is a lack of an entity that could address geopolitical disputes. This assumption is incorrect. Settling disputes between ‘geopolitical rivals’ is one of the main objectives of international law and its innumerable dispute settlement mechanisms. At the apex of the international legal order, the ICJ is tasked with deciding ‘in accordance with international law such disputes as are submitted to it’.⁵² In pursuit of this function, the ICJ addresses ‘geopolitical disputes’ frequently.⁵³ The argument here is not that the ICJ would, in principle, be the best entity to adjudicate upon cyberspace disputes. Depending on the factual circumstances of a given cyber incident, some fact-finding entities and tribunals (domestic, regional, international) might be better equipped than others. The argument is simply that the special cyberspace-related problem Smith claims to have identified (the lack of tools to address highly sensitive geopolitical disputes) is a problem international law handles every day. There is no doubt that the impartiality of existing judicial institutions tasked with addressing questions that engage sensitive State interests is threatened by the omnipresent necessity to retain State support. As a result, compromises need to be made and it could be argued that the international administration of justice is, sometimes, less ‘politically neutral’ than it could be. However, a novel attribution organization would face the same challenge. The effectiveness of such an organization would require the support of States who grant it access to potentially sensitive infrastructure and data.⁵⁴ The organization would need to tread as carefully as existing institutions and it is questionable if a private-led new organization would possess the ‘authority ... to face the political pressure resulting from ensuring State compliance to the regime of norms’.⁵⁵ If that is the case, the question arises as to what exactly a new organization could offer that existing institutions cannot.

⁵⁰ Ibid.

⁵¹ Wallace and Visger (n 25) 48.

⁵² Statute of the International Court of Justice (1945) 1 UNTS XVI art 38.

⁵³ See, eg, *Application of the International Convention of the Elimination of All Forms of Racial Discrimination (Georgia v Russian Federation)* (Preliminary Objections) [2011] ICJ Rep 70.

⁵⁴ Wallace and Visger (n 25) 50.

⁵⁵ Mariarosaria Taddeo, ‘Deterrence and Norms to Foster Stability in Cyberspace’ (2018) 31 *Philosophy & Technology* 323, 327.

Microsoft argues the distinguishing feature of the new organization would be the 'expertise of private sector technology firms'.⁵⁶ Technology firms likely possess a higher degree of technological expertise than certain States. But again, the field of cyberspace is not unique in that regard. Post companies and shipping operators presumably know more about their respective infrastructures, their vehicles and vessels than certain States. However, that does not mean that, based on that technical expertise alone, they should be entrusted with competences normally reserved to accountable public sector institutions.

Moreover, it is misleading to describe the process of attributing responsibility, which the new organization should engage in, as a mere technical procedure. Compared to fact-finding missions,⁵⁷ for example, attributing responsibility in a legal sense requires sophisticated analyses *inter alia* of chains of causation and of levels of intent. Rarely are conclusions black or white. When it comes to the activities of the IAEA, to which Smith referred, 'there is a clear demarcation between peaceful and non-peaceful uses of nuclear energy'.⁵⁸ However, 'there is not a similar clear-cut line in the cyber arena as the range of uses of cyberspace is much more varied than nuclear energy'.⁵⁹ When attributing cyberspace attacks facts would need to be interpreted and discretion would need to be exercised. These activities contain subjective elements. As such they are best left to entities that are accountable to those whose interests their decisions affect. In that regard, Microsoft's proposal to establish an unaccountable expert-staffed organization overlooks the fact that there 'is a clear tension between economic and technical legitimacy ..., and the international policy dimension of this legitimacy'.⁶⁰

Ultimately, the observation that there are shortcomings when it comes to identifying cyberspace perpetrators and attributing responsibility is correct. It is also true that one must think carefully about how international law's various dispute settlement mechanisms can be prepared in such a manner that they are able to deal competently with the challenges that cyberspace presents. However, it is doubtful whether a new private-sector led organization would be the most suitable response to these challenges. Calling for the establishment of

56 Microsoft (n 18) 1.

57 Although even the conclusions of fact-finding missions are frequently called into question. See, eg, The Guardian, 'Goldstone Report: The Unanswered Questions' *The Guardian* (5 April 2011) <www.theguardian.com/world/2011/apr/06/goldstone-report-unanswered-questions-editorial> accessed 9 January 2019.

58 Wallace and Visger (n 25) 50.

59 Ibid.

60 Louise Marie Hurel and Luisa Cruz Lobato, 'Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs' (2018) 3 *Journal of Cyber Policy* 61, 70.

a new organization despite the existence of international dispute settlement mechanisms is both inefficient and destabilizing. It is inefficient, because it forgoes the possibility of relying upon and of harnessing the vast amount of experience that existing institutions already possess. It is destabilizing because it calls the efficacy of existing norms and institutions into question. The proposal to establish a new organization might also underappreciate the potential for conflicts of interest that might arise between the objective of impartiality and the profit-maximizing rationale of technology sector enterprises. This problem is particularly pronounced with respect to Microsoft's third proposal.

3 The Global Technology Sector and the ICRC: An Imperfect Analogy

Towards the end of his speech, Smith invited his audience to 'look back [to] 1949 [when] the world's governments realized that they could not protect civilians in times of war without a private organization – the [ICRC].'⁶¹ In this spirit, Smith suggested that the technology sector should, as cyberspace's 'first responders',⁶² 'become a trusted and neutral Switzerland'⁶³ and 'sign [its] own pledge'⁶⁴ to 'assist and protect customers' and not to 'aid in attacking customers'.⁶⁵ Before considering why such a pledge would, in principle, be most welcome, it is important to address Smith's comparison of the technology sector with the International Committee of the Red Cross and the neutrality of Switzerland.

First of all, it should be noted, that it is inaccurate to observe that 'we don't have the same kind of organization [as the ICRC]'.⁶⁶ If there really is a parallel between the challenges that the ICRC was designed to address and the ones that the technology sector faces today, then it is not unthinkable that the ICRC could also be equipped with the necessary tools to treat victims of cyberattacks. That might not be an easy task, but with sufficient political support it would not be impossible. One might object that the ICRC was created to deal with situations that are fundamentally different. But that argument would merely confirm the argument presented here: that it is an imperfect analogy to compare the technology sector with the ICRC.

61 Smith (n 6) 11.

62 Ibid 4.

63 Ibid 12.

64 Ibid.

65 Ibid 13.

66 Ibid 12.

Furthermore, the technology sector differs from the ICRC in at least two respects. First, the ICRC is a not-for-profit organization whereas the technology sector is not. Second, the ICRC has no stake in a given battle, whereas the technology sector does.

With respect to the first difference, it cannot be ignored that technology companies are motivated by economic considerations.⁶⁷ Various statements from Microsoft make this clear. Smith explains, for example, that '[w]hen they [the Microsoft Threat Intelligence Center] spot a problem, they hand it off to our Cyber Defense Operations Center so they can go to work not only to protect our own *services*, but *customers* as well.'⁶⁸ Similarly, Microsoft's Vice President Scott Charney stated 'when one country attacks another country, ... for us, that's one *customer* attacking another *customer*'.⁶⁹ It is not objectionable that companies strive to maximize their profits. Indeed, they owe it to their shareholders to do so. However, motive matters. Dunant was acutely aware of this when he wrote in 1862 that '[f]or work of this kind, paid help is not what is wanted. Only too often hospital orderlies working for hire grow harsh, or give up their work in disgust or become tired and lazy.'⁷⁰ In other words, paid work is susceptible to be affected by countervailing interests. In cyberspace, such interests arise when corporate and humanitarian objectives do not align. For example, when a technology company is itself responsible for a cyberattack or for violating customer rights.⁷¹ Recently, in 2013, the Snowden revelations showed to which extent Microsoft was a 'willing collaborator in the NSA's surveillance program'⁷² and granted US authorities access to 'US' and foreign nationals' data'.⁷³ This is not to call the credibility of companies into question or to cast doubt on Microsoft's renewed commitment to protect the interests of its customers. But it does mean that it is problematic to equate 'profit maximizing technology firms with [a] humanitarian organization'.⁷⁴

67 Kristen Eichensehr, 'Digital Switzerlands' (Social Science Research Network 2018) SSRN Scholarly Paper ID 3205368 25 <papers.ssrn.com/abstract=3205368> accessed 4 January 2019.

68 Smith (n 6) 7 (emphasis added).

69 NYU School of Law, *Governing Intelligence: Panel 11: The New Transnational Oversight* <www.youtube.com/watch?v=3kTYMz-GSxA> accessed 4 January 2019 (emphasis added).

70 Dunant (n 1) 124.

71 Craig A Newman, 'When to Report a Cyberattack? For Companies, That's Still a Dilemma' *The New York Times* (6 March 2018) <www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html> accessed 9 January 2019.

72 Gorwa and Peez (n 26) 8.

73 Ibid 10–11.

74 Ibid 14.

The second difference between technology companies and the Red Cross is that the latter has no stake in any kind of battle. By contrast, technology companies are, in the words of Smith, ‘the plane of battle’.⁷⁵ The Red Cross societies are not the plane of the battle. Dunant ‘was a mere tourist with no part whatever in [the] conflict’.⁷⁶ Technology companies, however, literally supply arms to governments⁷⁷ and they maintain the infrastructure required to carry out cyberattacks. They are also, despite their efforts to create the impression that they ‘are on par with the governments that attempt to regulate them’⁷⁸ headquartered in States. As such they must submit to the ‘legal process and legal compulsion’ of any State ‘where they have assets and operations’.⁷⁹ The same cannot be said, at least not to the same extent, about humanitarian organizations like the Red Cross.

For these reasons, it is not desirable to compare technology companies with the Red Cross. Nonetheless, one should not dismiss Microsoft’s initiative outright. Entertaining the thought that the practices of private, profit-driven entities could amount to ‘soft-law’⁸⁰ is certainly going too far. However, it is most welcome that technology companies pledge to ‘protect customers’.⁸¹ In principle, the protection of customers should be a matter of course. It would hardly be acceptable for companies to explicitly reserve the possibility to facilitate attacks on customers and not to provide patches where and when they are needed. However, the frequent disregard that technology companies show for the interests of their customers,⁸² indicates that such a pledge might not be self-explanatory.

75 Smith (n 6) 4.

76 Dunant (n 1) 16.

77 See, eg, Joshua Brustein, ‘Microsoft Wins \$480 Million Army Battlefield Contract’ *Bloomberg* (28 November 2018) <www.bloomberg.com/news/articles/2018-11-28/microsoft-wins-480-million-army-battlefield-contract> accessed 5 April 2019; Scott Shane and Daisuke Wakabayashi, ‘“The Business of War”: Google Employees Protest Work for the Pentagon’ *The New York Times* (2 November 2018) <www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html> accessed 5 April 2019; Hayley Peterson, ‘The Pentagon Is Close to Awarding a \$10 Billion Deal to Amazon despite Trump’s Tweets Attacking the Company’ *BusinessInsider* (5 April 2019) <businessinsider.com/amazon-trump-wins-pentagon-contract-2018-4?r=US&IR=T> accessed 5 April 2019.

78 Eichensehr (n 67) 19.

79 Ibid 35.

80 Wallace and Visger (n 25) 54.

81 Smith (n 6) 12.

82 See, eg, Gabriel JX Dance, Michael LaForgia and Nicholas Confessore, ‘As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants’ *The New York Times* (18 December 2018) <www.nytimes.com/2018/12/18/technology/facebook-privacy.html> accessed 9 January 2019.

Perhaps most importantly, and despite the considerable unease expressed above with respect to Microsoft's proposed Digital Geneva Convention and a new attribution organization, it is positive to observe that international technology companies are aware of the political dimension of the work they engage in. One might not agree with the substance of the proposed suggestions, but the fact that companies like Microsoft unapologetically enter the political sphere also means that they open themselves up to public scrutiny and criticism of a political nature. This approach contrasts with the position of companies that seek to pre-empt critique of their activities by denying the political significance of their conduct. As an example of the assumption of bona fide corporate social responsibility Microsoft's proposals relating to the creation of a Digital Geneva Convention thus reflect a political self-awareness that is welcome.