GCSP
Geneva Centre for Security Policy
Where knowledge meets experience

JULY 2017 No. 4

STRATEGIC SECURITY ANALYSIS

The Proposed "Digital Geneva" Convention:

Towards an Inclusive Public-Private Agreement on Cyberspace?

by Maria Gurova

1 Introduction

On 14 February 2017 Microsoft president Brad Smith addressed[1] the participants of the RSA Conference in San Francisco with a passionate speech in which he called on all representatives of the private sector to unite their efforts to create a "digital Geneva" convention and digital "neutral Switzerland" regime. The initiative is inspired by the Geneva Conventions signed in 1949 in the aftermath of the Second World War and by Switzerland's longstanding tradition of neutrality. Considering the initiative's good intentions and the role Microsoft played in its creation, what lies behind this proposal, and has it emerged at the right time?

2 Why now?

In his address Smith presented six basic principles that lay the groundwork for a universal document for all private sector companies concerned with cyber security.[2] As the chief legal officer of a major company, he believes that, in the digital world, the "responsibility to protect" rests on the shoulders of the private sector with reinforcement from states. The principles reflect the major vulnerabilities that have become increasingly apparent in cyberspace, which have significant impact not only on the private sector in terms of financial losses, but mounting influence on international relations. Indeed, the rise of hacking incidents in the last two years is extremely disturbing. According to statistics,[3] 2016 saw the most hacking occurrences compared to the previous two years. In general, cyber crime costs the world economy around $400 billion[4] annually and is projected to reach $2 trillion[5] by 2019. Concerns are increasing about companies' and banks' vulnerability to cyber attacks.[6] The most recent cyber attacks using ransomware, for which public authorities do not have an effective solution, provide clear evidence of the need for cooperation between the private and public sectors in the cyber domain. Despite these grim statistics, however, collective private attempts have not been sufficient to deal with such attacks because of the diverging interests and competitive nature of the world market.

KEY POINTS

- Microsoft president Brad Smith's proposal that private sector entities should draw up and adopt a digital convention is timely, but risks being another exclusive coalition of like-minded actors without proper global outreach.
- In substance, the six principles of the proposed digital convention more closely resemble a mix of public and private international law than the principles of international humanitarian law, which are already applicable to the cyber domain, with some exceptions.
- Without support from the government sector and comprehensive outreach to the international community, any digital regime on a global scale will not be feasible.

1 B. Smith, "The Need for a Digital Geneva Convention", Official Microsoft Blog, 14 February 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/?subscribe=success#sm.000qydfow1dwnelksq411jnqswi9g.

2 Ibid.

3 Hackmageddon, "2016 Cyber Attacks Statistics", 19 January 2017, http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/.

4 McAfee and CSIS, *Net Losses: Estimating the Global Cost of Cybercrime. Economic Impact of Cybercrime II*, June 2014, https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

5 S. Morgan, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019", *Forbes*, 17 January 2016, https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#3843d7b93a91.

6 PricewaterhouseCoopers, *Global Economic Crime Survey 2016*, http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf.

There have been several attempts to reach an agreement – if not a legally binding one – that could unite at least public stakeholders and restrain malicious actors from encroaching on critical infrastructure and data. The Budapest Convention on Cybercrime[7], adopted by the Council of Europe in 2004, is the first binding agreement of its kind. Today, however, this convention is out of date. Recently, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) has made modest, yet significant progress. It managed to agree on a report[8] on norms and rules of behaviour in cyberspace and will be working on making financial infrastructure the focal point of steps to protect the cyber domain. For the most part, however, the documents referred to above recognise the dangers threatening cyberspace, but without introducing a binding mechanism to deal with them.

The North Atlantic Treaty Organisation (NATO) was the first organisation to make a collective effort to draft a document that could be regarded as a template for others to follow. NATO's *Tallinn Manual* series[9] is an ongoing analysis of cyber warfare and the applicability of international law to the cyber domain. Applicable only to NATO members, this series cannot be recognised universally, but it could be used as a template for a future binding set of rules. However, this is highly unlikely to happen because of the political differences between Western countries, on the one hand, and China and the Russian Federation, on the other.

Brad Smith's appeal is not the first call to the international community and the wider public to create an entirely new regime for cyberspace. However, it does offer a fresh take on the growing issue. The Geneva Conventions of 1949 have proved to be one of the most widely recognised legal documents in the world and have been signed by all countries, which is highly understandable, given the devastation caused by the Second World War and the importance of limiting warfare and protecting victims of armed conflicts. Although no international organisation can claim that its work is flawless or exceptionally efficient, due to high levels of bureaucracy, the International Committee of the Red Cross and Red Crescent (ICRC) has moved closer to reaching this goal than any other player in the field thanks to its clear humanitarian mandate. This may be the underlying reason for Microsoft's comparison between the cyber and real worlds. However, highlighting that the proposed digital Geneva convention should be based on the framework of the original Geneva Conventions and their Additional Protocols (which constitute the backbone of international humanitarian law (IHL), protect those suffering from war and regulate the conduct of hostilities during armed conflicts with the ultimate aim of limiting/preventing atrocities), Smith suggested a somewhat different set of principles, only slightly resembling those of IHL.

3 The six principles of the proposed digital convention

According to Microsoft, the proposed digital convention should base its legal power on six principles:

1. There should be no targeting of high-tech companies, the private sector or critical infrastructure.
2. The private sector should be assisted in its efforts to detect, contain, respond to and recover from cyber attacks.
3. System vulnerabilities should be reported to vendors rather than stockpiled, sold or exploited.
4. Restraint should be exercised in developing cyber weapons, and any that are developed should be limited, precise in their targeting focus and not reusable.
5. There should be no proliferation of cyber weapons.
6. Offensive operations should be limited to avoid mass and indiscriminate cyber attacks.

It is essential to note that IHL applies only in situations of armed conflict – and since Microsoft is suggesting the use of "Geneva Conventions language", everything the proposed digital convention covers should therefore fall within the framework

7 Council of Europe, Convention on Cybercrime, 23 November 2001, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

8 See United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 of 22 July 2015.

9 See NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, February 2017.

of an existing armed conflict – but whether a cyber incident could start an armed conflict and trigger the applicability of IHL is still highly debatable. Otherwise these situations would be covered by other branches of law (such as international human rights law) that provide even higher levels of protection than IHL.

From a legal standpoint, IHL consists of the four Geneva Conventions of 1949,[10] three Additional Protocols, other applicable treaties, and customary IHL covering international and non-international armed conflicts. Although significant, the Geneva Conventions are not the only source of IHL. To avoid getting bogged down in details, it suffices to point out that the first principle suggested by Microsoft is already covered by the principle of distinction in IHL, i.e. the distinction between combatants, and civilians and others who are *hors de combat* (out of combat, such as the wounded and sick). In Microsoft's first principle the private sector aims to be made the focal point of attempts to control cyber attacks and cyber crime, although it already benefits from IHL protection, like any civilian or civilian entity (as long as it does not participate in hostilities itself). Additional protection is indeed given to some categories of people and objects, such as hospitals, medical units and personnel, with IHL indicating specific concern for women, children, journalists, etc. What greater level of protection does Microsoft suggest, therefore? Additionally, in cases of full-scale hostilities between two entities, whether private or public, in cyberspace it would be extremely difficult to distinguish between combatants and non-combatants, unlike on real battlegrounds.

Microsoft's second principle resembles the central principle of the First Geneva Convention – the obligation to care for the wounded and sick – although it is slightly modified to accommodate the needs of the private sector. As for the third principle, this is a novelty, having no correlation with IHL principles. This idea may be inspired by trade law principles and is one of the more feasible elements that Microsoft suggests, because the public sector can assist private companies by outlining common areas for cooperation.

The other principles suggested for the proposed digital convention do not correspond to the Geneva Conventions and IHL, because cyber conflicts do not necessarily take the same form as actual warfare. The fourth and fifth principles closely resemble a non-proliferation regime, e.g. the Treaty on the Non-Proliferation of Nuclear Weapons[11] or the ongoing international campaign to ban nuclear weapons,[12] where the core message is explicit – albeit often contested – that parties to the treaty are required to prevent nuclear weapons proliferation. The fourth principle draws in part on Article 36 of Additional Protocol I,[13] which states that all newly developed weapons should comply with IHL. The ongoing development of new cyber weapons and the rise of "zero-day" forms of attack, in which the victim of a cyber attack does not have the capacity to shield itself from malware, have created a need to limit the development of new forms of cyber weapons. But this will unfortunately continue, however, due to the relative freedom of cyberspace and mounting social, political and economic gaps in society, coupled with the overall (and growing) socio-political turmoil of the modern period. Lastly, principle six is based on another well-established IHL principle, that of prohibiting indiscriminate attacks.

To deal with the issue of cyber crime, public representatives should establish close relationships with private companies in order to work together to reduce malicious cyber incidents and create efficient protective mechanisms and rules of the game. For example, in 2016 the European Union Commission signed an agreement[14] dealing with a public-private partnership on cyber security to establish a close working relationship between the two realms to tackle cyber-related threats. This initiative forms part of the Horizon 2020 plan to create a single digital market.

The UN GGE, whose mandate has been extended to 2017, has laid down norms and rules of behaviour in cyberspace, and is set to advocate for the protection of private sector banks as far as possible from potential cyber attacks as part of its further activities. In light of this, therefore, Microsoft is

10 See ICRC (International Committee of the Red Cross), *The Geneva Conventions of 1949 and Their Additional Protocols*, 1 January 2014, https://www.icrc.org/en/document/geneva-conventions-1949-additional-protocols.

11 See United Nations, *Treaty on the Non-Proliferation of Nuclear Weapons*, 1970, <https://www.un.org/disarmament/wmd/nuclear/npt/text/>.

12 International Campaign to Abolish Nuclear Weapons, "Voting on UN Resolution for Nuclear Ban Treaty", 23 December 2016, http://www.icanw.org/campaign-news/voting-on-un-resolution-for-nuclear-ban-treaty/.

13 ICRC, *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977.

14 European Commission, "Commission Signs Agreement with Industry on Cybersecurity and Steps up Efforts to Tackle Cyber-threats", Press Release, 5 July 2016, http://europa.eu/rapid/press-release_IP-16-2321_en.htm.

grounding its call not only in IHL, but also in customary law under the UN.[15] However, if the nascent digital convention is to be drafted to resemble laws such as the UN Convention on the Law of the Sea (UNCLOS), it is important to keep in mind that UNCLOS has state sovereignty deeply embedded in its principles, leaving only the "high seas" free from any sovereign rule or state control, instead stating that ships navigating the high seas are bound by the laws of the flag under which they sail. Here, the outcome is probably inevitable: cyberspace will not be regarded as being like the "high seas", where all actors can be involved and where only national rules and procedures will be applied. At most, states will grant such a privilege to the private sector.

The six principles suggested by Microsoft only borrow their wording from the concrete rules set out in the Geneva Conventions and IHL in general. The idea of using the Geneva Conventions and the ICRC to advocate for a new agreement on the use of cyberspace is reasonable from a public relations perspective, but the concept needs further elaboration and much more collaborative work among the parties concerned. In substance, these guidelines more closely resemble a mix of public and private international law rather than IHL principles alone, which in general are applicable to the cyber domain.

4 What might a future 'digital Switzerland' look like?

If the proposed digital convention aims to protect private sector and banking infrastructure around the world, incorporating non-proliferation principles into its core mandate is not the best solution, because many private companies are more concerned about guarding their corporate security and generating profits than establishing a framework of common rules, including on sharing confidential and potentially exploitable data. The cyber domain presents many challenges for attempts at legal regulation. In terms of applying the Geneva Conventions of 1949, which protect victims of armed conflict regardless of the parties involved and the cause of a particular conflict, ideally the conduct of the ICRC and other humanitarian organisations should be apolitical – which it is, for the most part. With private sector and cyber threats, however, impartiality of this kind is highly improbable. A potential "digital Switzerland" will never be neutral and detached from the politics and economics of modern life, of which the private sector is fully aware. The goal behind this suggestion, therefore, is to unite as many private companies as possible to create a precedent in international behaviour – i.e. to establish a norm – for others to follow. In today's public-private setting, however, this is not likely to happen, because large companies registered in countries like China, the Russian Federation and Turkey – where the private sector is not so private and depends on political relations with the authorities – will never be able to do this without falling out with their respective governments. If so, the suggested digital convention will only unite the private sectors of Western countries, creating yet another exclusive coalition of like-minded states.

As the main victims of cyber-attacks, countries and companies can work out guidelines for all the stakeholders involved. Tentatively, this is feasible through meticulous study of the existing norms of international law and IHL, which for the most part are applicable to cyberspace in its present form. Total protection of the private sector, as suggested by Microsoft, is well intended, but in reality is like building castles in the air. Alternately, private companies could suggest various areas for cooperation in order to reduce the risk of cyber-related incidents, e.g. like a recent initiative by Nokia, IBM, AT&T and other industry giants to create a cyber-security alliance.[16] This initiative will help to address difficulties experienced with the concept of the Internet of Things (IoT). Without attempting to impose a fixed set of rules, these companies will delegate their experts to explore the potential risks inherent in the IoT ecosystem. This is a promising example of how companies can unite their efforts without establishing a formal legal regime.

In principle, international law and IHL are applicable to the cyber domain, with some exceptions. Despite the fact that the principle of proportionality is well established in IHL, the matter of proportionate response in cyberspace – which is a difficult matter for countries to agree on – must be clear-cut and set in stone; unexplored areas, the development of new technologies and their incorporation into other aspects of life must be closely monitored. There is no likelihood that the public and private sectors will succeed without working together – willingly or not – in order to embrace this expanding reality of international relations. For decision-making bodies working on such issues, the opportunity to take the

15 See United Nations, *United Nations Convention on the Law of the Sea*, 10 December 1982, http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

16 G. Daniels, "IoT Cybersecurity Alliance launches with AT&T, IBM and Nokia", TelecomTV, March 2017, http://www.telecomtv.com/articles/iot/iot-cybersecurity-alliance-launches-with-at-t-ibm-and-nokia-14368/.

best from existing international conventions – including the Geneva Conventions – is immense. The non-proliferation regime should be the foundation for restraining a potential cyber weapons race, which could have devastating effects in the coming decades. As for Brad Smith's agenda, private companies must – and most likely will – work more closely together, but the prospect of creating such a regime with a separate legal organisation that will deal with private sector protection seems unlikely for now, due to the high level of political pressure and restraints on high-tech companies.

5 Conclusion

The "digital Geneva" initiative is undoubtedly a bold one, but the actual creation of such a regime is unlikely in the current international framework. The gap between the public and private sectors, national and international legal norms, and rules regulating cyber-related issues remains large, despite effort to bridge it. A potential legal regime to manage cyberspace should be flexible, reflecting the essential nature of the volatile cyber world. New technologies and the rapidly developing domain of artificial intelligence are having a growing impact on the international setting (including not only international organisations and the UN system, but international civil society), challenging international law. With some changes and wise combinations, stakeholders can avoid the burdensome business of creating new norms for the cyber world by adapting existing ones. Here, the private sector has a leading role to play, working together with public-sector representatives. Through its proposal, Microsoft has shown that such an initiative should be introduced to the wider public from the private sector, not imposed by state legal entities and authorities. In other words, it should be a bottom-up, not a top-down process.

About the author

Maria Gurova has recently worked as a junior policy analyst at the International Telecommunications Union. She previously worked for the Russian Federation International Affairs Council in Moscow as the programme coordinator in charge of the Russian Federation-US cyber dialogue project. She holds master's degrees from the Institut d'études politiques de Paris (Sciences Po) and Moscow State University of International Relations, as well as a certificate from the Geneva School of Diplomacy. In April 2017 she was part of the winning team in the GCSP-Atlantic Council Cyber Challenge 2017 in Geneva. She is interested in cyber security from a policy decision-making perspective.

Where knowledge meets experience

The GCSP Strategic Security Analysis series are short papers that address a current security issue. They provide background information about the theme, identify the main issues and challenges, and propose policy recommendations.

Geneva Centre for Security Policy - GCSP
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
CH-1211 Geneva 1
Tel: + 41 22 730 96 00
Fax: + 41 22 730 96 49
e-mail: info@gcsp.ch
www.gcsp.ch