A DIGITAL GENEVA CONVENTION?

THE ROLE OF THE PRIVATE SECTOR IN CYBERSECURITY

RAQUEL VÁZQUEZ LLORENTE

LSE !deas

STRATEGIC UPDATE

MAY 2018

LSE IDEAS is an IGA Centre that acts as the School's foreign policy think tank.

Through sustained engagement with policymakers and opinion-formers, IDEAS provides a forum that informs policy debate and connects academic research with the practice of diplomacy and strategy.

IDEAS hosts interdisciplinary research projects, produces working papers and reports, holds public and off-the-record events, and delivers cutting-edge executive training programmes for government, business and third-sector organisations.

 @lseideas

 facebook/lseideas

A DIGITAL GENEVA CONVENTION?
THE ROLE OF THE PRIVATE SECTOR IN CYBERSECURITY

RAQUEL VÁZQUEZ LLORENTE[1]

Cybersecurity has risen to the top of both national and international agendas. As the President of China, Xi Jinping, said in 2014, "without cybersecurity there is no real national security".[2] The first documented national security directive on communications and computer security was prompted by a Hollywood movie, War Games, that unsettled the then US President Ronald Regan already in 1983.[3] However, 9/11 and the 'War on Terror' ended up relegating cyberspace to a secondary security consideration.

The cyber-attacks against Estonia in 2007 brought some attention back to the digital territory, particularly around the legal aspects of cyber warfare and military operations. The boom of the digital economy and the datafication of businesses and society has now put the private sector at the center of cybersecurity debates. Recent data mismanagements, such as the breach that affected some 57 million Uber customers or the revelations that Facebook compromised the data of millions of their users, highlight the central role that the private sector plays in cybersecurity. Undeniably, corporations are key players in the digital realm—whether it is as distributors of malicious software, victims of cyber-attacks, or first responders to security breaches.

In this climate of cyber insecurity, Microsoft put forward last year the idea of a 'Digital Geneva Convention' to regulate cyber-attacks, sparking both criticism and support. This proposal exposes a fundamental question that has been long overlooked. What is the role the private sector should play in cybersecurity policy, and how can this co-exist with the traditional responsibilities of states?

THE CYBER WEAPONS MARKET AND THE MILITARISATION OF CYBERSPACE

The first part of understanding cybersecurity is grasping the breadth of the threat. The digital space has become a very crowded domain, with cyber threats coming from a range of sources.

The security company Symantec reported that they encountered 357 million variants of malicious software, or malware, in 2016. The market for malware is booming, and it caters to different budgets and purposes. A password-stealing 'Trojan' can be bought for as little as $25, while ransomware kits that freeze or steal files demanding a ransom can reach $1,800. Other offers include Distributed Denial of Service (DDoS) attacks, making an online service unavailable by flooding it with traffic from multiple sources. The fees vary depending on the target and the duration of the attack.[4]

Some firms have also found a market niche in offering intrusion products, which work by installing malicious software onto a device. UK human rights watchdog Privacy International's in-depth research of the global surveillance industry reveals 528 companies involved in the design and distribution of this technology—all located in traditional arms exporting states.[5] While malicious software is not new, the trade at commercial scale is.

Like any other underground market, the malware economy is difficult to estimate. Despite figures not being publicly available, researchers have made solid attempts at studying the market for cyber weapons, particularly those transactions concerning 'zero-day' vulnerabilities — flaws unknown to the software maker that can be then exploited until the weakness is found and patched.[6]

Edward Snowden's disclosures revealed that the US National Security Agency (NSA) uses and purchases zero-days, having budgeted in the past at least $25 million to purchase software vulnerabilities.[7] The CIA also maintains its own arsenal of cyber weapons, according to 8,761 files published by Wikileaks in March 2017. The vulnerabilities market is not only restricted to the US, though. At least Israel, Britain, Russia, India, Brazil, North Korea, Malaysia, Singapore, and Middle Eastern intelligence services also participate in the market as buyers.[8]

However, the most immediate cybersecurity problem is not the trade but the stockpiling of vulnerabilities. When state actors purchase software vulnerabilities and they do not inform the companies that have the capacity of patching them; users, economies, and societies become more vulnerable to hacking and cyber-attacks. When a vulnerability is kept secret, malicious actors can discover or steal it, and subsequently use it against any target of their liking or sell it. In addition, cyber

weapons differ from physical weapons in that when the malware is deployed, parts of the code can be repurposed and integrated into new malware that can even be more harmful than its predecessor.[9]

Large-scale cyber-attacks such as 'Stuxnet', the US-Israeli malware that caused the centrifuges of an Iranian nuclear plant to malfunction, or more recently 'NotPetya', which built on the ransomware 'Petya' that primarily attacked Ukraine, have put under the spotlight the role that states are playing in cyber arms proliferation. At the core is a tension between national security and public cybersecurity. 'Heartbleed', a major security vulnerability that was made public in 2014 and rose suspicions of having been earlier discovered by the NSA, prompted the White House to affirm that they have a bias towards disclosing vulnerabilities rather than stockpiling them.[10]

However, this policy was challenged last year by Microsoft in light of the NSA computer codes leaked by Shadow Brokers. Some of this malware, such as the exploit 'Eternalblue', which takes advantage of a vulnerability in a Microsoft protocol, was later partially incorporated into 'NotPetya' and 'Wannacry' cyber-attacks. The latter alone affected more than 150 countries, targeting among many others the National Health Service in the UK, power companies in Spain, a library in Oman, and the Norwegian soccer team. It is worth noting though, that according to the most comprehensive research to date, the figures of non-disclosed zero-days by the US Government are only in the single digits every year.[11] This discrepancy in the level of vulnerabilities stockpiles shows the opacity surrounding offensive cyber capabilities.

States are not only developing their own cyber arsenals, they are also creating cyber armies or funding loosely affiliated groups that can perpetrate sophisticated attacks. For instance, the Pentagon has increased its cyber staff from 1,800 people in 2014 to 6,000 in 2016.[12] China has built information operations units to research and deploy defensive and offensive cyber capabilities,[13] while Russia maintains a network of 'volunteers'.[14]

The intensification of states' activities is prompting reflections around the militarisation of cyberspace. Notably, during the Warsaw Summit of July 2016, NATO recognised cyberspace as a "domain of operations in which NATO must defend itself as it does in the air, on land, and at sea."[15] The US had already made such a declaration five years earlier.[16] Meanwhile, cybersecurity initiatives and budgets balloon to protect against some of the offensive capabilities that were originally developed, in many cases, by nation-states.

THE ROLE OF THE PRIVATE SECTOR IN CYBERSECURITY

A recent survey of 726 companies across 79 countries revealed that the threat of cyber-attacks is the biggest concern of businesses, from small firms to large corporations.[17] As the ex-CEO of Cisco put it "there are two types of companies:

those that have been hacked, and those who don't know they have been hacked".[18] While the estimates vary, the global cost of cybercrime was valued at $375-$575 billion in 2014.[19] With an increasing part of the global economy becoming digital, these costs will continue to grow, up to $2.1 trillion by 2019.[20]

Correspondingly, the rise of the global cybersecurity sector has also been significant in little more than a decade. In 2004, the global cybersecurity sector was valued at $3.5 billion,[21] it is now estimated to be at $135 billion.[22] In Europe alone, the $22 billion market is expected to grow at an 8% rate to 2018.[23] In the information age, securitising data has become a very lucrative business.

Corporations can fill different roles in cyber space, not only as responders to security breaches or victims of cyber-attacks, but also distributors of malicious software. Surveillance software sold by Israeli and European companies is gradually becoming a tool of choice by nations with poor human rights records. FinFisher, sold by the German company Lench IT, has been reportedly used in 25 countries to monitor political dissidents, activists, whistleblowers, and journalists.

The digital space is generally seen as a domain away from central control, however cyber policy, and in particular arrangements concerning digital tools, is being subsumed under the umbrella of military controls and foreign policy. The EU has incorporated a list of surveillance technologies into the sanction regimes for Syria and Iran, and the US has passed similar measures. At the global level, the current governance system of cyber weapons relies mainly on three instruments: the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (1996), the Budapest Convention (2001), and The Tallinn Manual.[24]

Intergovernmental organisations are also active. The OSCE has been leading the only project formally endorsed by states on confidence building measures—much in line with the history of the organisation in monitoring ceasefires and facilitating the exchange of information among militaries.[25] Similarly, information security has been on the agenda of the United Nations since 1998 as part of the Committee on Disarmament and International Security. However, the topic did not gain much traction until 2004, with the establishment of the UN Group of Governmental Experts (GGE).

This said, neither states nor corporations have yet come to terms with their multiple roles in cyberspace. The contribution of the biggest technology, software and cybersecurity companies—such as Apple, Alphabet, Oracle, IBM, Symantec, or Checkpoint Software Technologies—is generally limited to commenting on technical aspects, taking part in industry discussions, and proposing market-based solutions. For instance, the two sets of confidence building measures agreed by the OSCE to "reduce the risk of conflict stemming from the use of ICTs" include only a superficial mention to cooperation and engagement with the private sector.[26]

While a great deal has been written about the privatisation of security and war in the physical space, the role of the private sector in digital security and defense has been less noticed. This is even more striking given the unique nature of cybersecurity, as the infrastructure is predominantly owned and controlled by the private sector. Indeed, "future conflicts in cyberspace are very likely to be won or lost in the private sector, which runs, owns, and depends on the underlying networks and information, at least in the most advanced economies."[27]

MICROSOFT: AN EXAMPLE OF LEADERSHIP IN CYBERSECURITY POLICY?

The use of the Internet as a 'new battlefield' is a source of preoccupation for not only policy and decision makers, but also for key stakeholders in the private sector. The most outspoken and recent example among technology leaders is Brad Smith, Microsoft's President and Chief Legal Officer, who is calling for a 'Digital Geneva Convention' in the context of increased cyber-attacks perpetrated by nation-states. While the proposal has received mixed reviews in cybersecurity circles, it is important to understand first how a corporation got to position itself as such an important player in international security.

Microsoft's prioritisation of cybersecurity can be traced back to an internal memorandum circulated by Bill Gates in 2002, which changed the company's culture. The email, which is known as the 'Trustworthy Computing' memo, acknowledged the importance of placing security at the core of their products and created a team to move the initiative forward. The memo also mentioned the importance of gaining users' trust by promoting cooperation with other actors:

> "Trustworthiness is a much broader concept than security, and winning our customers' trust…it's a fundamental challenge that spans the entire computing ecosystem." [28]

Since then, Microsoft has positioned itself as a pioneering company in steering cybersecurity norms, institutions and principles which engagement is not limited to industry, but also decision and policy makers. In his testimony before the US Senate, the Vice-President of Trustworthy Computing called on the US government to "insist that the private sector be integrated into these international discussions" around cybersecurity norms.[29] Microsoft has also been an advocate for the internationalisation of the US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.[30] As a company present in virtually every country in the world, international cooperation among countries to implement similar laws and norms is vital for Microsoft to maintain its competitive edge in the market.

Microsoft has put forward a large number of proposals on cybersecurity—from industry only groups such as the Software Alliance, to 'transparency centers' aimed at serving governments. There are however, two proposals that epitomise Microsoft's

thinking on cybersecurity governance: the International Cybersecurity Norms and the Digital Geneva Convention (DGC).

THE DIGITAL GENEVA CONVENTION

Both the International Cybersecurity Norms and the Digital Geneva Convention span across multiple years and documents. The first white paper published in 2009, ***Rethinking the Cyber Threat: A Framework and Path Forward,*** introduced the language and ideas that would develop throughout four subsequent documents, to culminate in the Digital Geneva Convention. This first document outlined the nature of cyber threats and the categories of attacks and called for international cyber norms, understood as agreements on normal and acceptable behaviour, which the paper argued are "necessary and, ultimately, unavoidable".

The International Cybersecurity Norms and the DGC can be separated into two different proposals, but they are better understood as connected ideas influenced by contextual developments. There is a clear progression of Microsoft towards a more assertive approach on the need to regulate nation-states' behaviour in cyberspace. This evolution cannot be understood without three key developments: the uncovering of Stuxnet in 2010, Snowden's surveillance revelations in 2013, and the larger trend of increased attacks sponsored by nation-states.

While the initial proposition of creating cybersecurity norms was an attempt by Microsoft to regain control over an increasingly crowded digital space, the latest proposal of a Digital Geneva Convention is taking it a step further. The DGC is an umbrella term that encompasses three proposals: an attribution organisation that would analyse cyber-attacks and identify the perpretrators, an industry agreement to create a shared set of principles and behaviors that would protect citizens, and binding rules for nation-states.

As abovementioned, Microsoft's normative approach to cyber governance responds to market forces (customers will not buy products they cannot trust), however the DGC has three distinctive characteristics.

First, it revisits the traditional multi-stakeholder governance model of cyberspace by separating each stakeholder into designated action areas. States would be the signatories of the Digital Geneva Convention, whereas the private sector would commit to their own industry agreement, and an NGO would be in charge of investigating cyber-attacks. Current opposition to the DGC is mostly rooted in the fear that this will drive the current governance system—favorable to Western countries, and the US mostly—toward a multilateral approach, preferred by countries like Russia and China.

Second, the DGC employs humanitarian vocabulary and language similar to that used by civil society groups. Microsoft's responsibility in cyberspace has been a

common thread in past governance proposals, but the DGC furthers this notion by presenting Microsoft as a moral actor looking after the greater good of society. The DGC portrays cyber-attacks as a global humanitarian problem that can only be solved with the contribution of technology companies. Furthermore, it compares the role of IT companies to that of the Red Cross, insofar as they are often 'first responders' after a cyber-attack. Corporate statements on the DGC connect collective interest with shared concerns, positioning Microsoft as an actor with universal values. They draw comparisons not only to the Red Cross, but also to the United Nations and Switzerland's neutrality, and use expressions generally reserved to humanitarian advocacy. Microsoft argues that "we need to recognize that the time has come for us to come together as an industry around the world to call on the world's governments";[31] and call upon the moral duty of the technology sector:

> "We have brought the world together and it has put us in a position to forge perhaps almost a unique level of mutual understanding and respect for the needs of people around the planet".[32]

Third, the proposal is backed by senior leadership. Brad Smith, President and Chief Legal Officer of Microsoft, was in charge of unveiling the Digital Geneva Convention at the RSA Conference in February 2017, and since then he has published at least four articles in support of the idea and extensively campaigned for it at international meetings.[33] While previous statements on cybersecurity norms had been acknowledged by other stakeholders, they had never received the levels of attention of the DGC across different international fora. Following the announcement of the proposal, the US government[34] and NATO Cooperative Cyber Defence Centre of Excellence[35] pronounced themselves against it. On the other hand, some technology thought leaders gave their support.[36] In April 2018, a year after the DGC was first announced, 34 technology companies—including Facebook—signed up to the Tech Accord. Although it is notable the absence on the list of other tech giants such as Google, Amazon or Apple.

In sum, Microsoft's DGC not only normalises the participation and leadership of technology companies in global security arrangements but does so on a moral basis, by appealing to solutions that benefit society. Could this be "a revolution in policy-making, equal in its own way to the technological revolution that has sparked it"?[37]

CONCLUSION: WHAT ROLE FOR TECH GIANTS IN CYBERSECURITY GOVERNANCE?

The Digital Geneva Convention represents a new level of engagement unprecedented for a technology company. However, the proposal is flawed at least from an international law perspective. The DGC picks and chooses International Humanitarian Law principles and taglines at its convenience, without fully developing the concepts. For instance, it would have been more logical to introduce the notion of regulating cyber-attacks through the existing provisions that require states to ensure that new weapons, means or methods of warfare comply with international law. More strikingly, Microsoft proposes applying to peacetime conditions a convention that regulates war, while International Human Rights Law would be the applicable body of law—although the DGC is unclear about which exact situations is aiming to cover.

Despite the shortcomings of the Digital Geneva Convention, Microsoft's increased assertiveness in reaction to states' behaviour in cyberspace is a good opportunity to debate the role that the private sector should play in such a critical domain. Corporations "have, de facto, become part of the fabric of global governance."[38] Their role in cybersecurity governance has been, however, largely overlooked. Facebook's data breach and the subsequent use of the information by Cambridge Analytica to influence voters' decisions is only another example of the key position that technology giants play in global security issues, even if they are sometimes unwilling participants.

Ignoring the expertise and influence that the private sector has in technology policy will only compound the issues that arise from poor cybersecurity responses. In a global environment where the digital space has an ever-increasing role in national security, technology companies will need to play a more proactive role in the formulation of cybersecurity policies. We see this shift embodied in the Digital Geneva Convention. Determining which weapons can be used by nation-states is a field that has been out of bounds for the private sector, but we now have a company asserting its right to be part of the process—and quite successfully so.

It is time for decision-makers and governments to up their game so crucial global cybersecurity arrangements take in the expertise of the private sector, without elevating the role of technology companies to more than what they are—that is, stakeholders that respond mostly to market forces. ■

NOTES

1 This Strategic Update is based on the author's dissertation submitted in partial fulfilment of the requirements of the degree in International Strategy and Diplomacy (Master of Science), 2016-17.

2 Segal, A., 2016 (Ch. 2). ***The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age.*** [Kindle DX e-book]. New York: PublicAffairs.

3 Kaplan, F., 2016. ***Dark territory: the secret history of cyber war***. [Kindle DX e-book]. Simon and Schuster.

4 Symantec. 2017. ***Internet Security Threat Report. Government***. June 2017, Volume 22. [Online] [Accessed: 07 May 2018].

5 Privacy International. 2016. ***The global surveillance industry***. July 2016. [Online] [Accessed: 07 May 2018].

6 The most interesting works are: Fidler, M. 2015. "Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis". ***ISJLP***, Vol. 11, 405; Finklea, K 2017. "Law enforcement using and disclosing technology vulnerabilities". ***Congressional Research Service***. 26 April 2017; or Herr, T. 2017. ***Countering the proliferation of malware. Targeting the vulnerability life cycle***. Harvard Kennedy School Belfer Center for Science and International Affairs. Paper, June 2017.

7 Frei, S., 2013. ***The known unknowns: Empirical analysis of publicly unknown vulnerabilities***. NSS Labs Inc., Austin.

8 Perlroth, N. and Sanger, D.E., 2013. ***Nations buying as hackers sell flaws in computer code***. New York Times, 13 July 2013.

9 Denning, D. and Strawser, B.J., 2014. "Moral cyber weapons". In: Floridi, L. Taddeo, M. (eds.) ***The Ethics of information warfare***, pp. 85-103. Springer International Publishing.

10 Daniel, M. 2014. ***Heartbleed: Understanding when we disclose cyber vulnerabilities***. The White House, President Barack Obama, 28 April 2014. [Online] [Accessed: 07 May 2018].

11 Healey, J. 2016. ***The US Government and zero-day vulnerabilities***. Columbia SIPA [Online] [Accessed: 07 May 2018].

12 Breene, K. 2016. ***Who are the cyberwar superpowers?*** World Economic Forum, 4 May 2016. [Online] [Accessed: 07 May 2018].

13 Chase, M.S. and Chan, A., 2016. ***China's evolving approach to "integrated strategic deterrence"***. Rand Corporation.

14 Giles, K., 2011. ***"Information Troops" A Russian Cyber Command?***. CCDCOE Publications; also, Hulcoop, A., Scott-Railton, J., Tanchak, P., Brooks, M. and Deibert, R. 2017. ***Tainted leaks disinformation and phishing with a Russian nexus***. The Citizen Lab, 25 May 2017. [Online] [Accessed: 07 May 2018].

15 NATO. 2016. ***Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016***. Press release, para. 70, 9 July 2016. [Online] [Accessed: 07 May 2018].

16 DoD, US Department of Defense. 2011. ***Department of Defense strategy for operating in cyberspace.*** July 2011. [Online] [Accessed: 07 May 2018].

17 BCI, Business Continuity Institute. 2017. ***Horizon Scan.*** February 2017.

18 Chambers cited in PwC. 2017. ***Cyber security: European emerging market leaders***. January 2017. [Online] [Accessed: 07 May 2018].

19 CSIS, Center for Strategic and International Studies. 2014. ***Net losses: estimating the global cost of cybercrime.*** June 2014. [Online] [Accessed: 07 May 2018]

20 Moar, J. 2015. ***The Future of Cybercrime and Security***. Juniper Research, 12 May 2015 [Online] [Accessed: 07 May 2018].

21 Ross, A. 2016. ***Want job security? Try online security***. Wired, 25 April 2016. [Online] [Accessed: 07 May 2018].

22 Statista. 2017. ***Size of the cyber security market worldwide, from 2016 to 2021 (in billion U.S. dollars)***. [Online] [Accessed: 07 May 2018].

23 PwC 2017.

24 Stevens, T., 2017. "Cyberweapons: An emerging global governance architecture". Palgrave Communications, Vol. 3.

25 Grigsby, A. 2016. OSCE agrees to new confidence building measures. Pop the champagne?. Council on Foreign Relations, 31 March 2016. [Online] [Accessed: 01 May 2018].

26 OSCE. 2013. Decision no. 1106. Initial set of OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies. 975th Plenary meeting, 3 December 2013. [Online] [Accessed: 07 May 2018]. And OSCE. 2016. Decision no. 1202. OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies. 1092nd Plenary meeting, 10 March 2016. [Online] [Accessed: 07 May 2018].

27 Rattray, G. and Healey, J. 2010 (p.79). "Categorizing and understanding offensive cyber capabilities and their use". In: Dam, K. W. and Owens, W. A. (eds.), ***Proceedings of a Workshop on Deterring Cyberattacks***, pp. 77-97. Washington, DC: The National Academies Press.

28 Gates, B. 2002. ***Bill Gates: Trustworthy Computing.*** Wired, 17 January 2002. [Online] [Accessed: 07 May 2018].

29 Charney, S. 2012 (p.8). ***Written Testimony of Scott Charney Corporate Vice President, Trustworthy Computing, Microsoft Corporation.*** Senate Committee on Homeland Security and Governmental Affairs, Hearing on "Securing America's Future: The Cyber-Security Act of 2012". 16 February 2012.

30 McKay, A. 2016. ***Lessons from the NIST Cybersecurity Framework***. Microsoft Cybersecurity Blog Hub, 5 October 2016. [Online]. Also, Nicholas, P. 2017. ***NIST Cybersecurity Framework: building on a foundation everyone should learn from***. Microsoft Secure Blog, 7 June 2017. [Online] [Both accessed: 07 May 2018].

31 Smith, B. 2017 (p.9). ***The need for a Digital Geneva Convention***. Transcript of Keynote Address at the RSA Conference 2017. San Francisco, California, 14 February 2017 [Online] [Accessed: 07 May 2018].

32 ***Ibid***, p.15.

33 Smith, B. 2017. ***The need for a Digital Geneva Convention***. Microsoft Cybersecurity Blog Hub, 14 February 2017. [Online]; Smith, B. 2017. ***Growing consensus on the need for an international treaty on nation state attacks.*** Microsoft Cybersecurity Blog Hub, 13 April 2017. [Online]; Smith, B. 2017. ***The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack***. Microsoft On the Issues, 14 May 2017. [Online]; and Smith, B. 2017. ***We need to modernize international agreements to create a safer digital world***. Microsoft On the Issues, 10 November 2017. [Online] [All accessed: 07 May 2018].

34 Weber, .R. 2017. ***State Dept.'s top cyber official rejects call for 'Digital Geneva Convention'***. Inside Cybersecurity, 25 April 2017. [Online] [Accessed: 07 May 2018].

35 NATO CCDCOE. 2017. Geneva Conventions apply to cyberspace: No need for a 'Digital Geneva Convention'. 18 July 2017. [Online] [Accessed: 07 May 2018].

36 Notably, Eugene Kaspersky and Julian Assange. Kaspersky, E. 2017. ***A Digital Geneva Convention? A great idea***. Forbes, 15 February 2017. [Online]; Assange, J. 2017. ***Press Conference on CIA Vault 7Thursday 9:45 a.m.Tweet questions at #AskWLwikileaks.org/civ7p1***. Twitter, 9 March 2017. [Online] [Both Accessed: 07 May 2018].

37 Nicholas, P. 2017. ***Future-proofing principles against technological change***. Microsoft Secure Blog, 29 March 2017. [Online] [Accessed: 07 May 2018].

38 Levy, D. and Kaplan, R., 2008 (p.433). "CSR and theories of global governance: strategic contestation in global issue arenas". In: Crane, A., Matten, D., McWilliams, A., Moon, J. and Siegel, D.S. 2008. ***The Oxford handbook of Corporate Social Responsibility***, pp.432-451.

THE AUTHOR

Raquel Vázquez Llorente is a Senior Legal Advisor at eyeWitness, an organisation that works at the intersection of technology, law and public policy. In 2016 and 2017, she was featured in the Forbes '30 under 30' list for her contribution to the field of Law and Policy. She has also been nominated to the Choiseul 100 leaders of tomorrow. Raquel holds a degree in Law and Business Administration from Universidad Carlos III de Madrid and an MSc in International Strategy and Diplomacy from the LSE.

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

EXECUTIVE MASTERS PROGRAMME

INTERNATIONAL STRATEGY AND DIPLOMACY

LSE IDEAS, a centre for the study of international affairs, brings together academics and policy-makers to think strategically about world events.

This one year **EXECUTIVE MASTERS PROGRAMME** is at the heart of that endeavour. While studying in a world-leading university you will be able to learn from top LSE academics and senior policy practitioners.

The programme will sharpen your ability to challenge conventional thinking, explore new techniques for addressing risk and threats, and coach you in devising effective strategies to address them.

The course has been especially tailored so that you can accelerate your career while holding a demanding position in the public or private sector.

"Right from the first week I was able to apply the lessons I had learnt to our operational and policy work and to coach my teams to look at issues differently."

- Karen Pierce
British Ambassador
to the United Nations

CONTACT US

Email:
ideas.strategy@lse.ac.uk

Phone:
+44 (0)20 7107 5353
lse.ac.uk/ideas/strategy

A DIGITAL GENEVA CONVENTION? THE ROLE OF THE PRIVATE SECTOR IN CYBERSECURITY

RAQUEL VÁZQUEZ LLORENTE

Cybersecurity has risen to the top of the international agenda. This Strategic Update explores what role the private sector should play in the global policy response, with companies on the 'frontline' of the cyber threat often being more proactive than states.

For general enquiries:

Email: ideas@lse.ac.uk
Phone: +44 (0)20 7849 4918

LSE IDEAS
Houghton Street
9th floor, Towers 1 & 3
Clement's Inn
London, WC2A 2AZ

lse.ac.uk/ideas
twitter.com/lseideas
facebook.com/lseideas

Cover image remix source:
www.freepik.com