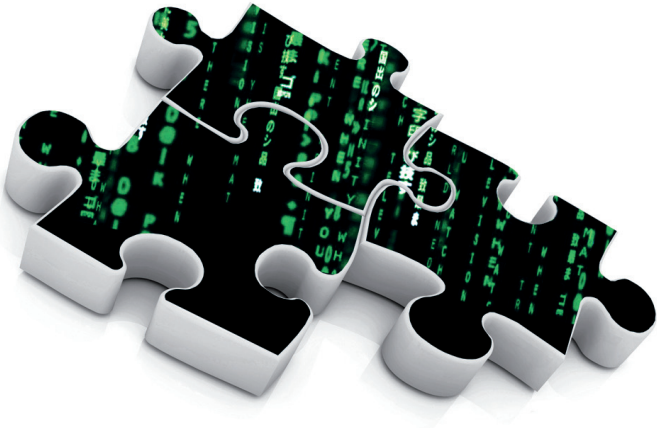


THE LAWS OF WAR AND CYBERSPACE

ON THE NEED FOR A TREATY CONCERNING CYBER CONFLICT

BENJAMIN MUELLER

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

STRATEGIC UPDATE 14.2
JUNE 2014

THE LAWS OF WAR AND CYBERSPACE

ON THE NEED FOR A TREATY CONCERNING CYBER CONFLICT

The existing international laws of war, known as the Law of Armed Conflict (LOAC), apply to all operational theatres, including cyberspace. International law distinguishes between two forms of aggression, both of which are impermissible under LOAC: the use of force, and armed attack. Absent an authorisation of force by the UN Security Council, only states under armed attack are legally allowed to deploy military force against another state.

Cyberspace is functionally distinct from land, air, sea and space. This distinction has a number of sources. First, cyberspace is the only man-made domain of warfare: the character of the domain space has been defined, and will continue to be defined, solely by human activity. Second, cyberspace is an intrinsically informational domain: it is used to create, organise, transfer, manipulate, assimilate and disseminate data. Cyberspace, in other words, consists of information and has an intrinsic informational *raison d'être*. It is a categorical mistake to treat the physical computing assets that sustain cyberspace as the domain of cyberspace itself.

This gives rise to confusions surrounding the role and applicability of the Law of Armed Conflict in cyberspace:

1. The gap between use of force and armed attack is already a contentious one, creating disputes about what level and kind of violence meets the 'armed attack' threshold. Cyberspace's unique properties dilute the meaning of these terms further: they enable non-violent electronic incursions – such as data theft, or systems sabotage – on a scale so vast that states' core security interests can be threatened, without any of the immediate kinetic damage traditional attacks produce.

2. Absent clear definitions of what constitutes an armed attack in cyberspace, states are likely to turn away from treaty-based conflict regulation and instead rely on more nebulous formulations based on national security instincts at best, and downright case-by-case evaluations at worst. This increases the chances of errors and miscalculations by state actors in cyberspace.

3. Conceptual confusions surrounding legal terms, in addition to low barriers to entry and attribution difficulties, give grounds to expect a marked increase in low-intensity cyber hostilities, at great cost to states and businesses, and with the potential to undermine trust in the Internet as a whole.

In response to these problems, this report calls on the international community of states to negotiate a body of law to regulate armed conflict in cyberspace. Internationally agreed-upon definitions on cyber use of force, cyber attack, and cyber espionage will provide the clarity needed to anchor states' expectations of military behaviour in cyberspace. Otherwise, states' cyber operations will increasingly push boundaries of the acceptable in order to tease out the limits of what can be gotten away with: states will resort to proxy combatants, digital camouflage and other acts of perfidy in order to circumvent constraints on armed conflict that were developed in a non-digital era.

Cyber hostilities are not the only source of security threats on the Internet: cyber crime is an equally destabilising force. Because attribution is difficult in a digital context, identifying and holding accountable actors in cyberspace is challenging. The most difficult hurdle, however, is not technical: the central problem is insufficient law enforcement cooperation between states. An intergovernmental body that institutionalises such collaboration will strengthen states' efforts to tackle the scourge of Internet crime. Cyber criminals hide behind the international legal barriers erected by sovereignty which their arena of crime – the Internet – does not heed. Placing a positive duty on states to help each other prosecute cyber crime has the added benefit of reducing the incentive for states to outsource illegal cyber war operations to 'cyber militias' that operate at arm's length: non-cooperation by a government during the prosecution of cyber perpetrators can be taken as evidence for joint culpability.

Cyberspace is a shared military and civilian domain. If the military dimension gradually evolves into a zone of perpetual low-intensity combat, the integrity of civilian cyberspace will steadily erode away. This report makes two recommendations to avert that scenario:

1. The community of states needs commonly agreed-upon legal standards to define what constitutes an illegal armed attack in cyberspace.

2. The community of states needs to establish an obligation for mutual assistance in cross-border cyber crime investigations.

These two steps, if implemented, ought to introduce a degree of order and certainty to cyberspace and, as a corollary, enable the serious prosecution of cyber criminals who currently take advantage of limited intergovernmental legal cooperation in cyberspace.

INTERNATIONAL LAW CONSTRAINS HOW STATES WAGE WAR

There exists a relatively comprehensive framework of norms that governs both the process of going to war and conduct in war. States generally adhere by these rules. Certain categories of weapons are banned outright and others are strictly controlled; the use of force by one state against another is outlawed unless it is for self-defence; rules differentiate between legal and illegal operations and strategies in war.

New technologies put a strain on these legal understandings as states establish the compatibility of a novel weapon with existing laws of war. Air power provides a good example of this. As with the Internet, airplanes were first used for intelligence gathering before the military potential – inflicting massive damage to enemy territory through aerial bombardments – was recognised, including the threats it posed to civilians. The day the Second World War broke out in Europe, Franklin D. Roosevelt cabled all warring parties asking for a public pledge that their air forces would not intentionally target civilian populations. England, Germany, France and Poland all agreed, and, as one opponent of international cyber law states, 'they tried to honour their pledges'.[1] This informal agreement lasted almost a full year, despite it not being codified in treaty law. It collapsed because of the ruthlessness of German military strategy: after the Luftwaffe destroyed the entire old city of Rotterdam in May 1940, Britain retaliated in kind over the Rhineland, and the war in the skies quickly became unlimited.

The attempt to define the permissible scope of aerial combat in the Second World War shows that states are willing to establish communal norms of warfare and try to follow them. Two powerful dynamics act against the rationale of complying with the laws of war: the military logic of the technology in question, and the absence of enforcement mechanisms. Circumscribing a technology's military utility creates incentives for cheating, giving a unique strategic advantage to defector states, especially if there is no way to punish cheaters. Nonetheless, nations were and are willing to work out rules of war that benefit all parties, to sign up to them, and to try to comply. The key is to frame pragmatic rules that work, and to monitor compliance through a permanent institutional mechanism, the absence of which undermined the airpower agreement in the Second World War. The Nuclear Non-Proliferation Treaty, for example, has proved a successful legal instrument to curtail the spread of nuclear arms, preventing this class of weapons from becoming a commonplace tool in the arsenal of states.

1 Baker, Stewart A. and Charles J. Dunlap. 'What is the Role of Laywers in Cyberwarfare?' *American Bar Association Journal*, May 2012

International legal norms surrounding war have meaning: most states try to abide by them, and they also exert significant efforts to signal to the international community that they do so.[2] All the evidence suggests that states, by and large, observe the international treaties they subscribe to, a principle known as *pacta sunt servanda*. As American legal scholar Louis Henken put it in 1968, 'almost all nations observe almost all principles of international law and almost all of their obligations almost all the time'.[3] Henken made this observation at a time when international law, after the terrible events of the Second World War, became an increasingly influential component of the thickening web of international relations in a globalising age, spearheaded by political institutions such as the UN and technocratic multilateral organisations such as GATT. Whether coincidentally or not, inter-state warfare became less and less common in this era of a growing, solidifying international legal order.[4] At best, international law facilitated this laudable trend, at worst it didn't preclude it. In any event, LOAC has provided a degree of clarity and a global normative convergence regarding impermissible state behaviour.

CYBERSPACE IS A UNIQUE DOMAIN THAT CHALLENGES CONVENTIONAL UNDERSTANDINGS OF USE OF FORCE, ARMED ATTACK AND ESPIONAGE

Cyberspace arises out of the Internet, the global set of interlinked computer data networks that are used for both physical and ideational purposes.[5] The name 'cyberspace' is given to the digital data trail generated by interconnected computers. While cyberspace cannot be spatially located, it gives rise to 'real' effects. The contrast to other operational theatres is simple: cyberspace cannot be reduced to physical attributes only. It is partially a material domain, used for commercial activities (e.g. e-banking) and infrastructure management (e.g. industrial control systems), and partially an ideational domain – a platform for information exchange and communication. In 1984, William Gibson published *Neuromancer*, one of the formative works of the cyberpunk genre that anticipated many features of the computer age we now take for granted. Gibson metaphorically styled cyberspace as 'a consensual hallucination experienced daily by billions … Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.'[6] More prosaically, the Congressional Research Service defines cyberspace as 'non-physical terrain created by computer systems'.[7] Cyberspace expresses human thought in data and allows it to manipulate – through computers and other humans – the physical world.

2 Koh, Harold H. 'Why Do Nations Obey International Law?' *The Yale Law Journal* (1997) Vol. 106

3 Henkin, Louis. *How Nations Behave*. New York, NY: Columbia University Press, 1968

4 For the decline in inter-state war, see Gleditsch, Nils Petter, Peter Wallensteen, Mikael Eriksson, Margareta Sollenberg, and Håvard Strand. 'Armed Conflict 1946-2001: A New Dataset.' *Journal of Peace Research* (2002) Vol. 39

5 Michael Benedikt formally defined cyberspace as "a globally networked, computer-sustained, computer-accessed, and computer-generated, multidimensional, artificial or 'virtual' reality" in *Cyberspace: First Steps*. Cambridge, MA: MIT Press, 1994

6 Cited in Jagoda, Patrick. 'Speculative Security,' in Reveron, Derek (ed.), *From Cybersecurity to Cyberwar*. Washington, D.C.: Georgetown University Press, 2012

7 US Congressional Research Service. 'Cyberwarfare.' (RL30735; June 19, 2001) by Steven A. Hildreth.

This nebulous complexity is the root reason why we struggle to answer basic questions of military doctrine such as, 'When does a cyber operation amount to the use of force?' After all, such operations need not result in immediate physical destruction. This legal haze surrounding cyber operations confuses the categorisation of incidents, and, by extension, the determination of legitimate responses. The Agent.btz malware discovered by the NSA in 2008 provides a good example of the problem.[8] Agent.btz, a spying programme, infected the Secret Internet Protocol Router Network used by the State and Defense departments to transmit classified material, and the Joint Worldwide Intelligence Communication System through which Top Secret information is sent to US officials across the globe. To remove Agent.Btz the military launched Operation Buckshot Yankee, which ended up lasting 14 months. This entailed the escalation of US Strategic Command's information security threat level, since programmes used by battlefield commanders for intelligence and communications were implicated in the clean-up. Agent.btz was a purely data-related cyber incursion, but one of such a vast scale that it destabilised military command and control systems and threatened to cross the boundary between espionage mission and outright attack. An intense conceptual debate began among the various affected US government agencies concerning the nature of what they were dealing with: did the US experience a military attack, requiring a response in kind by the military's offensive cyber unit at the time, Joint Functional Component Command? Or should the incident be treated as an act of espionage, albeit on an enormous scale? In the event, policy officials opted for the latter interpretation. Agent.btz demonstrated the difficulty of treating cyberspace like any other operational domain: cyber security and intelligence operations overlap. Unlike non-cyber espionage, cyber incursions can be mounted against other states remotely and scaled up to such a degree that they implicate core national security concerns. Such incidents can be likened to covert military operations. Interpreting international law in this novel context is enormously difficult.

The official policy of the United States is that the Law of Armed Conflict (LOAC) applies to cyberspace, since all new technologies are subject to existing laws of war.[9] Conceptually, however, there are strong reasons to suspect that cyberspace should be subject to a discrete body of law.

The clarity of the concepts relied on by the Law of Armed Conflict is diluted in cyberspace The LOAC restricts the use of military force between states: Article 2(4) of the United Nations Charter outlaws the use of force against the territorial integrity of another state, and Article 51 of the Charter entitles a targeted state to respond against an armed attack with its own, proportionate use of a force. US doctrine in the event of

8 For an in-depth report, see Nakashima, Ellen. "Cyber-Intruder Sparks Massive Federal Response — and Debate Over Dealing with Threats." *The Washington Post*. 09 Dec. 2011. Web. 22 Mar. 2014.

9 See Koh, Harold H. 'International Law in Cyberspace.' *Harvard International Law Journal* (2012) Vol. 54

a cyber intrusion is to assess its physical effects.[10] A cyber operation is a use of force, the US government maintains, if its scale and effects are comparable to non-cyber uses of force. Specific criteria are used to determine whether the use of force threshold is breached by a cyber operation: the context of the event, the actor perpetrating the action, the target and location, effects and intent.[11] Such an effects-based analysis of cyber attacks considers serious death, injury, damage or destruction as the threshold for an armed attack. US government policy further states that any cyber use of force can be deemed an armed attack, triggering the self-defence provisions of LOAC.[12]

The central ambiguity of the LOAC rests on the distinction between the use of force and armed conflict. Contesting interpretations of the two categories makes the question of a breach of *jus ad bellum* difficult enough outside of a cyber context: all armed attacks constitute use of force, but not all uses of force are armed attacks.[13] Whether an incident breaches the armed attack threshold determines whether force can legally be applied in self-defence. This gap in the LOAC's response structure has existed long before cyberspace came about, but cyber conflict exacerbates the issue: it adds to the interpretative complexity of LOAC, and widens the zone of ambiguity surrounding the rules.[14] Ultimately, the question of whether a cyber operation amounts to a use of a force and whether the armed attack threshold has been breached 'depends on a holistic assessment of the incident in light of attendant circumstances'.[15] In the absence of an internationally negotiated and sanctioned code of what is militarily permissible in cyberspace, such ad hoc legal assessments provide a fragile basis for international law to constrain the militarisation of cyberspace.[16]

It is easy to conceive of cyber operations that bring about enormous disruption to an economy or lead to data theft on such a scale as to endanger national security. Take the following two scenarios:[17]

(i) A state bombs the stock exchange building of another state at night. There are no casualties. A physical back-up and business continuity plan are in place. Trading is not disrupted.

10 For a discussion of just how such assessments are made, see Schmitt, Michael N. (Ed.). *Talinn Manual on the International Law Applicable to Cyberspace.* Cambridge: Cambridge University Press, 2013

11 See Schmitt, Michael N. 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed.' *Harvard International Law Journal* (2012) Vol. 54

12 Koh, *International Law in Cyberspace*; see also Sofaer, Abraham D. 'International Law and the Use of Force.' *American Society Of International Law Proceedings* (1988) Vol. 420

13 See Schmitt, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed'

14 Fidler, David P. 'Economic Cyber Espionage and International Law.' *American Society of International Law Insights*, (2013) Vol. 17, p. 27

15 Schmitt, 'International Law in Cyberspace' p. 20

16 Ibid, p. 27

17 Based on Lin, Herbert S. 'Offensive Cyber Operations and the Use of Force.' *Journal Of National Security Law & Policy* (2010) Vol. 4

(ii) A state launches a cyber attack against the stock exchange of another state at night. There are no casualties. The back-up is also compromised electronically and the business continuity plan fails. Trading is disrupted for a week.

These scenarios, designed to tease out the complexities of warfare in cyberspace, sit uneasily with the international laws of war. The first attack, owing to the physical destruction of a building, constitutes a use of force; the second attack brings about far greater economic damage, but, lacking a kinetic element, does not amount to a use of force. Therein lies the rub: the legal definitions of war do not reflect the full reality of combat in the cyber era.

The issue is not that international law is inapplicable to cyberspace: it is rather the unique nature of cyber activities, which can bring about destructive results without concomitant physical injury or damage.[18] As Agent.Btz showed, cyberspace enables the scaling up of purely informational operations to the degree where states may feel their national security is under threat, even in the absence of a conventionally understood attack that produces immediate physical damage. Cyber hostilities are obscure: they occur electronically, involving lines of code as weapons; they need not (but can) create proximate kinetic effects, need not (but can) be launched remotely without any physical violation of the target state's sovereignty and need not (but can) result in enormous loss of data and/or critical command and communications infrastructure.

Considerable legal opacity surrounds such an obscure operational environment. Unless the laws of war are updated to accommodate new cyber realities, this state of affairs invites calamity. A continuing definitional vacuum creates a destabilising interpretative uncertainty and sets up an 'offensive incentive': it encourages offensive operations that endeavour to undershoot the 'use of force' threshold. Since this threshold is ultimately in the eye of the beholder, it is a matter of time before one state's cyber espionage is another state's cyber attack. If the line between spying and attacking in cyberspace has to be clarified retrospectively, it may be too late: the law needs to be one step ahead, not behind.

18 Schmitt, p. 37

THE KEY TASK FOR STATES IS TO FORMALLY DISTINGUISH BETWEEN CYBER EXPLOITATION AND CYBER ATTACK, AND TO OUTLAW THE LATTER

There are two main conceptual categories of cyber operation.[19] The first is cyber exploitation, which is a non-destructive action, typically clandestine, that seeks to obtain information that would otherwise remain confidential. The second is cyber attack, which is a deliberately destructive action that aims to alter, disrupt, deceive, degrade or destroy adversary computer systems or networks or the information resident in these systems or networks, whether clandestinely or not. In cyberspace, exploitation is a pure data acquisition mission, while an attack seeks to destabilise the adversary's computer systems and networks, causing it to be unavailable or untrustworthy and therefore less useful to the adversary.[20]

Espionage in a cyber context is a vexing issue. All states engage in the clandestine acquisition of confidential intelligence from other actors. The digital age has neither created nor changed this goal. What has changed, however, is the means available to states by which to achieve it. Whereas traditional espionage necessitated some kind of direct physical interaction with the target state, cyber espionage can be conducted without the perpetrator ever leaving their home state. This renders such intelligence work immune to the method used to tackle traditional espionage, namely, through target states' domestic legal systems. Moreover, it has given spies the ability to scale up the rate and volume of data theft in a way that was hitherto unimaginable. In 2010, the director of the NSA called the loss of information and intellectual property through cyber espionage 'the greatest transfer of wealth in history', suggesting that states are beginning to see their core national security concerns affected by this dynamic. The line between espionage and covert operations is blurry in cyberspace, which is one of the reasons that it needs to be firmly drawn. States have historically been reluctant to treat espionage as anything other than a domestic law enforcement concern.[21] This is because it is a useful practice employed by all states.[22] In fact, insofar as it reduces information asymmetries between states, espionage can have a calming effect on international relations.

---

19 The following definitions are based on Lin, 'Offensive Cyber Operations and the Use of Force'. See also Lin, 'Operational Considerations in Cyber Attack and Cyber Exploitation' in Reveron (ed.), Derek (ed.), *From Cybersecurity to Cyberwar*

20 In technical terms, what distinguishes the two is the payload of the attack: an exploit accesses data, an attack affects functionality. A cyber exploiter seeks to compromise the confidentiality of protected information afforded by a computer system or network; an attacker seeks to degrade the system's integrity. For a taxonomy of various cyber attacks and exploitations see Lin, 'Operational Considerations'

21 The fact that states have been unwilling to outlaw or even codify espionage is evidence for the relevance of international law: states only sign such treaties when they actually intend to adhere to them. For that reason, Israel is not party to the Nuclear Non-Proliferation Treaty; and Syria only joined the UN Chemical Weapons Convention in October 2013.

22 Knake, Robert K. 'Untangling Attribution: Moving to Accountability in Cyberspace.' Prepared statement to the US House of Representatives Committee on Science and Technology. *Planning for the Future of Cyber Attack*. July 5 2010. Accessed at < http://www.cfr.org/united-states/untangling-attribution-moving-accountability-cyberspace/p22630> See also Lin, 'Offensive Cyber Operations and the Use of Force,' 78; Scott, Roger D. 'Territorially Intrusive Intelligence Collection and International Law.' *Air Force Law Review* (1999) Vol. 46, p. 217

Clarifying the meaning of armed attack and use of force in cyberspace has the added benefit of implicitly charting out the legitimate scope of other, national security-related clandestine cyber activity.

It is not immediately clear what the implications of cyber espionage are for the LOAC. Cyber espionage is not inhibited by the costs, consequences and limitations of traditional espionage.[23] At the same time, espionage is not typically considered a hostile act. Opinions differ as to what the best strategy is to cope with digital espionage. Entities like the CIA argue that cyber espionage does not fall under the umbrella of cyber war, since the US government, like all governments, conducts network surveillance and has done so since the advent of electronic communications. One solution is to develop norms that accept the necessity of espionage, but recognise the potential for boundless digital espionage to do severe damage to trust between states, and limit the extent to which states engage in it.[24] Another is to distinguish strictly between cyber operations that capture data, and those that alter the intruded network in a way that affects their functionality now or in the future.[25] A further option is to tackle industrial espionage by expanding the provisions of the WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights. Currently, member states are obliged to protect certain intellectual property rights and trade secrets within their territories, but not in their operations abroad.[26]

In 2009 the Wall Street Journal reported that Russia and China had breached the US electric grid and introduced malware with the potential to disable it, and that US intelligence agencies had detected successful cyber attacks against other states' critical infrastructures.[27] It is unclear whether the article is accurate or not, and it is also not reported whether the US has undertaken similar such operations. But in any case, even if it is not immediately destructive, the pre-emptive penetration of an adversary's critical infrastructure is dangerous, destabilising and undermines trust between states. This situation – where cyberspace is used to launch attacks against other states' civilian infrastructure, including the introduction of cyber vulnerabilities in critical infrastructure by stealth – is an example of the kind of cyber operation that sits uneasily with existing concepts and needs to be clearly defined as an illegal act of aggression.

It is for states to negotiate the specifics of any supplementary international laws of war that pertain to cyberspace. The overriding aim must be to address the definitional deficiencies of existing LOAC addressed above. The zone of ambiguity as regards cyber exploitation vs. attack vs. espionage, and use of force vs. armed attack, must be shrunk as much as possible.

---

23 See Knake, 'Untangling Attribution,' p. 6
24 Ibid
25 See Oona Hathaway et al. 'The Law of Cyber-Attack.' *California Law Review* (2012) Vol. 817
26 See Fidler, p. 30
27 Gorman, Siobhan. 'Electricity Grid in the US Penetrated by Spies.' *The Wall Street Journal*. April 8, 2009. Web. Accessed 22 March 2014

NEW MILITARY TECHNOLOGIES TEST THE STRENGTH OF EXISTING LAWS

Nuclear weapons were never formally outlawed under international law. What kept the peace between the US and the USSR was a volatile mixture of deterrence and an arms race. This worked because any nuclear attack could easily be traced to the aggressor and would be followed by symmetric retaliation; hence the apocalyptic name of this doctrine, Mutually Assured Destruction. Moreover, only a small number of states ever developed nuclear weapons, in part due to the technological challenges involved therein, but mostly because early mover states set about institutionalising a formal regime of non-proliferation to prevent the uncontrolled spread of nuclear weapons. This is not a possibility for cyber weapons.

Under current policy, cyber warfare is treated as subject to existing international law, like other new technologies that preceded it, such as nuclear weapons. But, as discussed, the military utility of the digital revolution is different: operations in cyberspace are diffuse, difficult to attribute, exhibit low barriers to entry, and are impossible to deter without explicit procedural frameworks (i.e. international law) that govern responses to such attacks. Where nuclear technology brought about deterrence, cyber operations incentivise offence, at least in the absence of a clear and credible definition of what amounts to the use of force in cyberspace.[28] This report therefore makes the case that explicit protocols of international law in cyberspace ought to be developed and enshrined in treaty law, in order to update definitions and concepts of aggression and war that made sense in the pre-digital world, but are dangerously ambiguous and vague in a digital context.

We have already witnessed military operations in cyberspace that has been deemed offensive by some states and acts of nuisance by others. A widely cited cyber operation against Estonia in 2008 crippled the country's telecommunications infrastructure, creating serious and widespread disruption of the country's financial and communication systems. It was initially characterised by Estonian officials as an armed attack, giving the country the right to military self-defence. NATO allies, faced with the possibility of being dragged into a military conflict, interpreted the attack differently. It is difficult to slot cyber operations into LOAC's legal categories, a task that would be greatly aided if internationally agreed-upon definitions were drafted. Clearly, international lawyers would not be facing similar issues in the event of a nuclear attack. [29]

In the absence of a consensus on what counts as illegal offense and legitimate defence in the cyber domain, states will be tempted to push the boundaries of the acceptable. Former NSA and CIA Director Michael Hayden was blunt about this dynamic:

28 See Andres, Richard B. Andres, 'Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence' in Reveron (ed.) *Cyberspace and National Security*

29 See Fidler, David P. 'Inter arma silent leges Redux? The Law of Armed Conflict and Cyber Conflict' in Reveron (ed.) *Cyberspace and National Security*

> 'We are moving from a world in which most cyber problems are mainly about stealing your data to a world in which cyber is being used to deliberately create direct kinetic consequences: effects on your information, effects on your networks, and other adverse physical effects on assets that are valuable to you. As surely as night follows day, these cyber security risks are going to expand over time.'[30]

In short, we can expect cyber operations to proliferate – a trend that has already begun[31] – until the day a targeted state decides that LOAC has been breached and responds accordingly. If clear legal constraints on cyber operations are set up now, this potentially disastrous scenario can be averted.

THE OPERATIONAL SUCCESSES ACHIEVED IN CYBERSPACE ARE IMPRESSIVE, BUT SHOULD NOT BLIND US TO THEIR CONSIDERABLE DANGERS

Some spectacular operations have taken place in cyberspace. Stuxnet, for example, was a successful cyber attack that set back Iran's nuclear programme by multiple years.[32] Is it really sensible to deprive our militaries of what appears to be an effective delivery channel for operations that do not entail full-scale warfare? Focusing only on the operational success of cyber missions neglects the wider strategic picture. Stuxnet achieved no more than a temporary delay in Iran's nuclear programme. At the same time, it implicitly legitimised this kind of cyber sabotage. So it was in a sense only a matter of time before a retaliatory mission would succeed. This eventually occurred in the form of a cyber attack on Saudi Aramco's internal computer network, rendering 30,000 computers inoperable.[33] While oil production remained unaffected, this episode was a worrying taste of the kind of tit-for-tat, gradual escalation of tensions in cyber that needs to be avoided. If this dynamic continues unchecked, cyberspace will become increasingly militarised. And it mustn't be forgotten that cyberspace is a shared military and civilian arena. The civilian portion depends on a large degree of trust and confidence in the integrity of the network for it to function properly. It is in all of our interests to prevent cyberspace from turning into a battlefield in all but name. This does not equate to outlawing all offensive uses of cyberweapons – it means clarifying what can and cannot be done military in cyberspace, thus ending the current free-for-all.

30 Joye, Christopher. 'Transcript: Interview with former CIA, NSA Chief Michael Hayden.' *Australian Financial Review*. 19 July 2013. Web. Accessed 22 March 2014

31 Watts, Sean. 'Low-Intensity Computer Network Attack and Self-Defense.' In Pedrozo, Raul A. and Wollschlaeger, Daria P. (eds.). *International Law and the Changing Character of War*. International Law Studies Vol. 87, 2011

32 Arimatsu, Louise and Mary Ellen O'Connell. 'Cyber Security and International Law.' *Chatham House International Law Meeting Summary*. 29 May 2012

33 See Bronk, Christopher and Tikk-Ringas, Eneken. 'The Cyber Attack on Saudi Aramco.' *Survival: Global Politics and Strategy* (2013) Vol. 55

IF STATES AGREE TO ASSIST EACH OTHER IN CYBER LAW ENFORCEMENT AS A MATTER OF ROUTINE, CYBER ATTACKS BY PROXY ACTORS ARE UNLIKELY AND CYBER CRIME CAN BE PURSUED MORE VIGOROUSLY

Even if such international law does come about, states can still engage in prohibited acts, because it is nearly impossible to prove culpability in cyberspace. It is a legitimate worry that the difficulties in attributing cyber operations make the enforcement of international law more challenging. Contrary to popular belief, however, attribution is not so much a technical issue as one of lack of international cooperation.[34] Security professionals are almost always able to build a fairly comprehensive investigative case after an attack, through a mixture of technical forensics and traditional intelligence work.[35] In this day and age, such investigations can even be undertaken by non-governmental entities.

Last year, the security company Mandiant published an exhaustive report on China's main army unit conducting operations in cyberspace, down to identifying the very building that houses the unit in question and even some of its individual operatives (who were identified because they had used their computing skills to circumvent China's Facebook ban).[36]

Even the most mysterious of cyber incidents carry traces of authorship. The main obstacle to successful attribution is that states don't cooperate with each other's inquiries as a matter of routine. If an organisation is set up by treaty to facilitate cross-border law enforcement in cyberspace – an Internetpol, so to speak – and signatories accept a positive duty to assist other signatories' law enforcement inquiries for specified crimes, the incentive for states to conduct offensive cyber operations at arm's length through proxy actors is reduced. Following the aforementioned cyber incursion against Estonia, for example, the investigating agencies were able to trace the origin of the attack to Russia. The Russian government, however, simply refused to co-operate with the investigation, and no effort was made to track down the culprits.[37] Attribution by non-cooperation ought to therefore be included in the body of international cyber law that this report suggests should be drafted. If uncooperative states are assumed to share culpability in an attack that can clearly be traced to their borders, states will have a strong incentive not to engage in such behaviour. Lower standards of attribution make sense in cyberspace by putting states on the line and encouraging them to rein in unauthorised operations by cyber militias.[38]

---

34 Knake, 'Untangling Attribution', p.5

35 So it was, for instance, with the Agent.btz attack. See Stewart, Phil and Wolf, Jim. 'Old Worm Won't Die After 2008 Attack on Military.' *Reuters*. 17 June 2011. Published online. Accessed 22 March 2014 at <http://uk.reuters.com/article/2011/06/17/us-usa-cybersecurity-worm-idUSTRE75F5TB20110617>

36 Mandiant. *APT1 - Exposing One of China's Cyber Espionage Unit*. 18 February 2013. Published online. Accessed 22 March at < http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>

37 Shackleford, Scott J. 'From Nuclear War to Netwar.' *Berkeley Journal of International Law* (2009) Vol. 27, p. 208

38 International law is malleable in this regard. The International Court of Justice opted for a high standard for attribution in *Nicaragua v. United States* (complete dependence of the operation on a nation state) while

The result of all this will be a degree of regulation in military cyberspace, which then allows states to devote more energy to a task that concerns them all equally: cyber crime. Far too little effort is spent prosecuting cyber criminals, who cleverly take advantage of the barriers of sovereignty. Conducting operations in other jurisdictions, they are currently safe in the knowledge that cross-border prosecution is such a complex endeavour that it is unlikely they will ever face justice.[39] The global cost of cyber criminality may be as high as $1 trillion per year.[40]

50 states have so far signed the Council of Europe's Convention on Cybercrime, also known as the Budapest Convention. This is the only binding international instrument that seeks to tackle Internet criminality. Its signatories include all of the members of the Council of Europe bar Russia, as well as the US, Japan and Australia. The Budapest Convention synchronises national laws on cyber criminality, which facilitates cross-border cooperation. It has done much to improve the prosecution of borderless cyber crimes, especially through provisions such as a 24/7 points of contact network between parties to expedite assistance requests; the requirement to preserve evidence at the request of another party which can then follow up with a request to search, seize, or disclose that data; and the positive duties on parties to harmonise investigative procedures and legal frameworks of cyber crime. Most categories of cyber crimes are covered by the Convention.[41]

However, parties can refuse cooperation if they deem that providing assistance would prejudice their sovereignty, public order or other 'essential interests'. Moreover, there is no enforcement mechanism to oblige states to fulfil their cooperative duties. Straightforward improvements of the Convention would include circumscribing the grounds for refusing assistance to other parties, and reforming the Convention's current dispute resolution mechanism to provide for mandatory reviews by a neutral arbiter whenever a party whose assistance request has been denied asks for one.[42]

---

the International Criminal Tribunal for the former Yugoslavia established a lower attribution threshold in *Prosecutor v. Tadic* (overall control of the operation by a nation state). See Fidler, 'Inter arma silent leges Redux'; International Court of Justice, 'Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits,' *ICJ Reports* (1986); International Criminal Tribunal for the Former Yugoslavia, *Prosecutor v. Dusko Tadic* (1999) Case No. IT-94–1-A

39 See, for instance, Bhattacharjee, Yudhijit. "How a Remote Town in Romania Has Become Cybercrime Central." *Wired Magazine*. 31 Jan. 2011. Web. 22 Mar. 2014.

40 Myrli, Sevrre. 'NATO and Cyber Defence.' *NATO Parliamentary Assembly Commmittee Reports 2009*. 173 DSCFC 09 E BIS. Web. Accessed 22 March at <http://www.nato-pa.int/default.asp?SHORTCUT=1782> It is difficult to obtain such statistics, because companies are likely to under-report these kinds of incidents – after all, prosecution is unlikely while reputational costs are high. The benefits of to systematically going after cyber criminals are enormous: as anyone participating in e-commerce can attest, the pervasive threat of crime adds substantial layers of cost and complexity to doing business on the Internet. See, for instance, Binham, Caroline. 'The Hacker Hunters.' *Financial Times Magazine*. 21 November 2013.

41 The full text of the Convention is available at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

42 National Research Council. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, DC: The National Academies Press, 2010

INTERNATIONAL COOPERATION OVER THE PROSECUTION OF CYBER CRIMINALS FACILITATES TRUST BETWEEN STATES, MAKES THE INTERNET MORE SECURE, AND CREATES THE BASIS FOR A MEANINGFUL LEGAL FRAMEWORK FOR STATE CONDUCT IN CYBERSPACE

Countries such as Russia and China, suspected of orchestrating state-sponsored or state-tolerated cyber incursions, are not party to the Convention. Russia, however, has on multiple occasions called for an international cyber arms control treaty. Specifically, it has called for the prohibition of inserting malicious code in another country's computers for use in the event of war, the prohibition of attacks on noncombatant networks and other restrictions on the military use of cyber weapons.[43] In 2010, NSA Director Keith Alexander responded to Russian prompts on the matter, agreeing on the need to 'establish the rules [for cyber warfare] and I think what Russia's put forward is, perhaps, the starting point for international debate'.[44]

The overall aim is to move the international community of states into a position where cyber-related cross-border cooperation of law enforcement is a matter of routine, regulated by treaty. An accord on cyber war is needed to clarify the definitions of LOAC in cyberspace, helping to bring clarity into what is currently an under-regulated domain of warfare. By creating a degree of certainty as regards permissible state behaviour in cyberspace, governments can step away from the risky game of maximising cyber operations without breaching the armed attack threshold, and focus on the scourge of cyber criminality, which is undermining confidence in the Internet as a whole. An institutionalised basis for international cooperation on cyber crime would make life harder for cyber criminals. As an added benefit, a treaty on cyber crime would lessen the attribution dilemma, since non-cooperation by a state can then be seen an indication of a degree of state responsibility for a cyber incident.[45] In practical terms, it is up to states to initiate the treaty process. The Budapest Convention provides a solid basis for combating cyber crime; it could be amended as per the points above and an effort launched to bring on board more signatories.

The UN Disarmament & International Security Committee appears to be the most appropriate forum for talks to commence on a cyber war treaty. The incentive structure for states to engage in such a process is easily framed in the game theory terms that are familiar to students of bargaining and cooperation under anarchy.[46] The simplest explanatory analogy is the Prisoner's Dilemma: it is in the interest of all

43 See Kramer, Andrew E. and Markoff, John. 'U.S. and Russia Differ on a Treaty for Cyberspace.' *The New York Times*. 27 June 2009. Web. 22 March 2014

44 Transcript of Remarks by Gen. K. Alexander at the Center for Strategic and International Studies, Washington, D.C. (June 3, 2010) at 11, available at <http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf>

45 National Research Council. *Proceedings of a Workshop on Deterring Cyberattacks*

46 The seminal work here is Axelrod, Robert and Keohane, Robert. 'Achieving Cooperation Under Anarchy – Strategies and Institutions.' *World Politics* (1985) Vol. 38

states if cyberspace becomes a more ordered military domain, by anchoring expectations and introducing a degree of certainty for governments. It is in the private interest of each state to defect from this regime and secure the benefits of unrestrained cyber warfare on its own. To avoid all states from following their private interest and defecting, it is necessary to monitor compliance, ideally through an institution charged with this task (which generates what Axelrod and Keohane call the 'shadow of the future'). Curiously, although international law has no formal enforcement mechanism, states' adherence to it, as has been noted, is widespread and consistent. The reasons are likely to be a mixture of enlightened self-interest in an ordered international community, legitimacy (both of international law and of the compliant state in the eyes of its population as well as the international community) and the norms of socialisation that have built up over the past century as international law grew in depth and breadth.[47]

The main hurdle facing this scheme is that states fear giving up a military advantage – a fear that is nullified if all states sign up to the treaty – and the worry that regulating a decentralised, non-hierarchical network like cyberspace is antithetical to its fundamental purpose. Specifically, concerns have been voiced that regulating cyberspace will generate momentum for those states that seek to exert censorship and state control over the Internet.[48] The idea that information is free, with the Internet as the medium to decentralise the global flow of knowledge and empower citizens across the globe, is indeed appealing to those who believe in freedom of speech as a fundamental force for good in the world. At the same time, it is easy to romanticise this point. Whether or not citizens enjoy a 'free web' still depends first and foremost on the domestic legal situation in which they find themselves. A state intent on censoring the Internet can do so easily, with or without a treaty on cyber war. What advocates for an open Internet seem to miss is that a key ingredient of the web is trust between the disparate nodes and actors in the network. A gradual militarisation of cyberspace will hamper cyberspace's effectiveness as a tool for commercial and social exchange. Moreover, the arms race dynamic that can develop absent a treaty on cyber war is a boon to cybercriminals, who, if left unchecked, will make e-commerce an increasingly slow, costly and cumbersome affair. That is in nobody's interest.

47 Koh concludes his famous review article, 'Why Do Nations Obey International Law?', with the following passage: "'Why is it,' Oran Young asked in 1992, 'that an actor acquires and feels some sense of obligation to conform its behavior to the dictates or requirements of a regime or an institution? ... I think that there are differences in being obligated to do something because of a moral reason, a normative reason and a legal reason.' Although Young did not further specify, I would argue that these moral, normative, and legal reasons are in fact conjoined in the concept of obedience. A transnational actor's moral obligation to obey an international norm becomes an internally binding domestic legal obligation when that norm has been interpreted and internalized into its domestic legal system. Both Franck and the Chayeses, exemplars of the philosophical and process traditions, respectively, recognize that transnational actors are more likely to comply with international law when they accept its legitimacy through some internal process."

48 For an overview of the debate, see Gross, Michael Joseph. 'World War 3.0' *Vanity Fair* (May 2012). Web. Accessed 22 March 2014

CONCLUSION

Technology and war have always coexisted in an uneasy juxtaposition, each feeding off the other, creating the basis for both humanity's progress and for awful, bloody setbacks. A century after the outbreak of World War I, it is worth remembering that one of the reasons why the war assumed such monstrous dimensions was that strategists had been blithe about the impact of technological progress. Machine guns, tanks, gas, aeroplanes and modern warships unleashed a degree of carnage that was simply not anticipated in advance by war planners.[49] The danger we face today is that digital technology is not tamed through social norms, and the world sleepwalks into a future where aggressive state behaviour in cyberspace causes increasing damage and ill-will among nations. Military strategists have been busy adapting their force structures to the cyber era, but the evolution of war's legal standards lags behind.

Humanity has a tendency to learn lessons *post hoc*, but good policy-making is as much about proactively mitigating against bad consequences before it is too late. Because success here is measured by the absence, not presence, of an event, such policy is harder to sell. This report aims to achieve such a 'sell' by highlighting the inadequacies of existing LOAC in cyberspace, and suggesting potential principles for a future body of international law concerning conflict in cyberspace.

Any zone of ambiguity in the law, history and logic teach us, will be exploited by states operating in an insecure environment. Currently, this zone of ambiguity in cyberspace is large, but it can be narrowed. That is the task that statesmen face.

Cyberspace is functionally distinct from all other military domains (air, sea, land and space). It isn't just a physical but also an informational realm. And because of the close proximity of kinetic operations (resulting in physical damage of the kind that LOAC was designed to regulate) and espionage operations in cyberspace, the lines between armed attack, the use of force and intelligence operations are blurring. We need a specific set of definitions that clarifies cyber hostilities. Currently there is no internationally agreed upon set of standards regarding what counts as an armed attack in cyberspace. This increases the likelihood of misunderstandings that can unintentionally lead to conflict. It also incentivises offensive tactics in cyberspace, as states push the boundaries of the acceptable in order to test other states' commitment to defend their national security, and their strategies for doing so.

49 See, for instance, Macmillan, Margaret. *The War That Ended Peace*: *How Europe Abandoned Peace for the First World War*. London: Profile Books, 2013. P. 5

In an era in which the meaning of armed attack is diluted by the presence of a new operational domain with novel properties, it is imperative that clear constraints on state behaviour are established. The worry that states will end up conducting cyber-attacks at arm's length through proxies, allowing them to disavow responsibility later, is legitimate. By creating a legal responsibility to assist law enforcement enquiries by victim nations, such states will be forced to show their hands one way or another.

By design, the Internet relies on a firm bedrock of trust for its optimal operation. Common protocols, mutual identification and the security of encrypted data transmission are necessary and sufficient conditions for commerce and other exchanges to take place on a disparate network like the Internet lacking a 'Leviathan', or central overseer. If insecurity and aggression become defining features of the Internet, it will lose most of its potential as a force for good in the world. By contrast, if cyberspace no longer presents an arena of warfare with unclear rules, and militaries can approach this domain with a degree of regulatory certainty, then states can focus their energies on pursuing cyber criminals. The world will be better off for it. ■

the **Author**

Benjamin Mueller is the Stonex PhD scholar in International Relations at LSE IDEAS. He holds a BA in Politics, Philosophy and Economics from the University of Oxford and a MSc in International Relations Theory from LSE.

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 top 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
UK's Permanent Representative to the UN and WTO in Geneva

CONTACT US

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

THE LAWS OF WAR AND CYBERSPACE

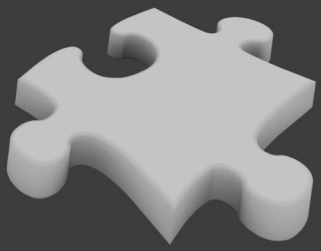
ON THE NEED FOR A TREATY CONCERNING CYBER CONFLICT

For general enquiries:
Email: IDEAS.reports@lse.ac.uk
Phone: +44 (0)20 7849 4918

LSE IDEAS
Houghton Street
London WC2A 2AE
United Kingdom

lse.ac.uk/ideas

This report examines the militarization of cyberspace and considers ways to prevent the Internet from turning into a battlefield. Cyberspace is a domain of warfare unlike all others: it is primarily informational in nature, accessible electronically without the need for spatial proximity, and acts as a global data and communication highway. These properties have given rise to highly unusual patterns of continuous, low-intensity clandestine cyber conflict. The existing Laws of War, which apply to cyberspace as a matter of doctrine, are ill-equipped to deal with this. The community of states must negotiate a treaty on cyberwar, institutionalise cross-border law enforcement cooperation of cybercriminals, and place state-sponsored digital espionage within the World Trade Organisation's remit to arbitrate anti-competition disputes. Absent these steps, the Internet will become increasingly militarised, international cybercrime will continue to elude serious prosecution efforts, and the web's utility for commercial and civilian purposes will degrade over time.



Cover image credits
Mostafa Fawzy,123RF Stock Photo; yourwallpaper.com