Cyberattacks and Cyber Conflict: Where is Conflict Resolution?

Monika Wohlfeld and Jack Jasper

Introduction

In this paper we analyse cyberattacks and cyber conflict and the challenges they pose to the field of conflict resolution. State and non-state actors alike are conducting cyberattacks in new and sophisticated ways that result in conflicts which are not readily addressed by conflict resolution approaches. Consequently, these developments in cyberspace take place without much input from conflict resolution scholars and practitioners.

We suggest that these developments in cyberspace result in changing relationships between actors, and thus potentially different types of conflict, based around two key problems. First, there is the problem of attribution. Cyberspace is inherently linked with anonymity and attributing a cyberattack with certainty is almost never possible. In addition, it is difficult to distinguish the difference between various types of actors, which include a mixture of states, non-state groups, and individual hackers.

Second, conditions in cyberspace overwhelmingly incentivize offensive strategies as opposed to defensive. Perpetrators can operate with no warning, and target specific weak spots, whereas cyber defences must be constantly monitored and updated to remain effective. It has been argued that timeframes for responding to a cyberattack are shortened, especially in situations that require negotiations.[1] The consequences of a failed attack are few, and the potential rewards are valuable.

With so much potential for conflict stemming from these new developments, one might expect the conflict resolution field to focus on them. And yet, a cursory appraisal of the relevant literature produces almost no results. We suggest that the field needs to address these issues on two fronts. First, it needs to do this through the formulation of new models and adjustment of existing models, for example third party mediation, negotiation, and intervention. Second, conflict resolution must join in the discussion of prevention and

responses to cyberattacks and cyber conflict. Specifically, we envisage engagement with technical experts to better understand current realities and likely developments in the near and short term, as well as instilling conflict resolution values in policy approaches, technical developments, and national and global governance.

This argument will be presented as follows: first, as cyber terminology varies widely across the literature, relevant definitions will be provided. We do not go into detail, though we do point to various sources for further reading. We will then provide a brief outline of how various actors have committed cyberattacks and engaged in cyber conflict. These will underscore the two problems identified above. Next, we highlight the response of certain states and international organizations to the threat of cyberattacks and cyber conflict. In the following section, we link the debate to the field of conflict resolution, focusing on what is and is not currently being done in practice, and make suggestions for urgent action. Finally, we conclude with some brief remarks on what was discussed in this paper and some reflections on the future.

Defining cyberattacks and cyber conflicts:

Arguably, cyberattacks are recorded daily. In addition, coordinated campaigns of cyberattacks conducted by state and non-state actors are resulting in cyber conflicts, which are different from their physical counterparts, but nonetheless have implications beyond cyberspace. The terminology is virtually endless when it comes to cyber-related issues, and we do not wish to be bogged down in the quagmire of definitions. For the purposes of this paper, we adopt roughly the same definition of a *cyberattack* proposed by Hathaway et al., that is, "any action taken to undermine the functions of a computer network for a political or national security purpose."[2] Cyberattacks may provoke a *cyber conflict*, which Valeriano and Maness define as "the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities short of war and away from the battlefield."[3] Cyber conflict would thus be differentiated from a cyberattack based on its emphasis on changing the relationship between two or more entities.

Much debate surrounds the prospect of "cyberwars" (which Thomas Rid defines as "potentially lethal, instrumental, and political acts of force conducted through malicious code"[4]) and whether they are currently happening or will happen in the future. Journalistic accounts of the current realities often refer to cyberwar or cyberwarfare when, in fact, they

are discussing cyberattacks and cyber conflict. Scholarly literature occasionally uses interchangeable terms to describe the same events. We acknowledge that there is the potential for such wars occurring, but in this paper largely focus on the experience with cyberattacks and cyber conflicts to date. To avoid speculation, we do not address that part of the debate. Hybrid wars, which will be discussed in the following section, are included in our analysis as they involve the use of cyberattacks alongside conventional military weapons.

New cyber developments to date

This section refers to several new developments related to cyberattacks and cyber conflict. Largely these entail the involvement of non-state actors as both state operatives and as distinctive players in addition to state actors and ultimately the emergence of so-called hybrid wars. These developments present two interconnected problems. The first is attribution, which is inherently difficult to determine because actors in cyberspace operate almost (but arguably not entirely) anonymously.[5] Some states take advantage of this fact by utilizing non-state actors to further obfuscate their involvement.

(i) The Attribution Problem:

The reliance of some states on non-state actors as conduits of their national security strategies in cyberspace best exemplifies the attribution problem. Even if a state government is believed to be responsible for orchestrating a cyberattack, there is almost no way for that to be proven in a timely manner, if at all.[6] In the event that attribution is eventually determined, the use of non-state actors affords states plausible deniability. As an example, Russia has been implicated in recent cyberattacks in Estonia, Kyrgyzstan, Lithuania, and Georgia, as well as alleged election meddling in the United States and a number of European Union member states[7] and denies having done so. Such activity is made possible by incorporating so called *hacktivists* into the national security strategy, a policy which some suggest is followed by Russia, but also China, North Korea, Iran and other states.[8]

So-called hacktivists are hackers that operate in cyber space with a political motive; they do not always work in conjunction with state officials. When hacktivists do work under the direction of state officials, they typically are organized in a collective, which is referred to by some as a cybermilita.[9] The obvious advantage to utilizing cybermilitias is that it further removes state officials from responsibility. However, their use of non-state actors is not without its drawbacks. The overarching strategy or objective may be handed down from

state officials, but the implementation of the cyberattack falls on the hacktivists themselves, who are not accountable to a government, and are essentially free to determine the means of meeting their objective. If a cyberattack were to go too far, thus eliciting a response from the target state, suspicion may be enough to warrant a military response. Escalating conflict may be an unintended consequence. The section below on responses to cyberattacks and cyber conflict addresses this further.

Hybrid wars are characterized by the "[incorporation of] a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder"[10] in pursuit of the achievement of political objectives. Jacobs and Lasconjarias argue that "hybrid warfare most often involves non-state actors such as militias, transnational criminal groups, or terrorist networks. These non-state actors are in many cases backed by one or several states, in a kind of sponsor-client or proxy relationship."[11] The cyber aspect of hybrid wars has become much more sophisticated since the concept of such wars was first developed in the early 2000s.[12]

To provide an example, the Kosovo conflict of the late 1990s has been labelled as the first "Internet War" due to tactics adopted by a pro-Serbian group known as the Black Hand. NATO, the United States, and the United Kingdom were all subjected to distributed denial of service (DDoS) attacks, which overwhelm networks with massive amounts of requests, as well as receiving malware-infected emails of various strains.[13] The result was not overly severe – NATO's website was intermittently down for a few weeks – but the trend towards hybrid wars has continued.[14]

Much literature has been devoted to the study of violent non-state actors in recent years, a category that includes transnational criminal organizations, terrorist groups, insurgency and guerrilla movements, and paramilitary groups, among others. Typically, these groups will form in states that lack legitimacy and the capacity to enforce its authority over its entire territory.[15] Cyberspace presents a new domain through which violent non-state actors can extend their reach beyond the borders of the states in which they operate.

Though its physical presence appears to be on a decline since a peak in 2014 and 2015, it is reported that ISIS has now shifted its approach to focus on cyber capabilities.[16] Under the new banner of the "United Cyber Caliphate," ISIS is able to pursue a strategy of online

recruitment and cyberattacks. Though unconfirmed, ISIS is thought to be making use of hacking tool kits that have themselves been stolen via a hack of Equation Group, a subcontractor for the US National Security Agency.[17] Once these sorts of tools are purchased or stolen, they become available to anyone on the web who knows where to look and with the means to purchase them.

(ii) The Incentivization of Offensive Strategies:

The second problem is that such an environment incentivizes offensive strategies over defensive ones. Attribution plays a role, as some have argued that when it is difficult to determine the perpetrator of a cyberattack in general, the magnitude of retaliation (or threat of retaliation) must be correspondingly high for effective deterrence.[18]

Offence is also significantly easier than defence. Indeed, in 2018, the President of the German internal security agency (Verfassungsschutz) opined that Germany is subject to cyber sabotage efforts by other countries, which aim to place specific programs in critical infrastructure to be ready for offense. In this view, Germany thus has no option but to use preventive offensive actions and must be ready to damage the enemy before an attack takes place.[19] Because cyber defences will always have vulnerabilities, they are constantly in need of maintenance and updates, which is a costly expenditure. Richard Andres argues that this further incentivizes pre-emptive offensive attacks, as cyber defences will constantly be probed in order to determine new vulnerabilities.[20] These offensive probes are relatively cheaper than maintaining cyber defences.[21] The result is a modern manifestation of the classic security dilemma in which technological developments occur at a rapid pace.

Responses to cyberattacks and cyber conflict

Responses of states and international organizations to the above developments have varied, but virtually all have sought to acknowledge the threat of cyberattacks and cyber conflict within their respective security strategies. States have unsurprisingly developed specialized agencies and devoted resources to expand their capacity to operate in cyberspace. In 2014, the International Telecommunication Union, as a specialized agency of the United Nations (UN), presented the Global Cybersecurity Index, which aimed to measure the commitment of states to cybersecurity.[22] In the 2017 edition, the index found that only 38 percent of states had a formalized cybersecurity strategy, while 12 percent were in the process of developing one.[23] This section lays out a small number of examples of how states and international

organizations grapple with the issue. We argue that, among those states that seek to formulate responses to cyberattacks and cyber conflicts, some have taken steps towards a cooperative approach and considering de-escalation possibilities, but most securitize the issue and focus on steps that can be understood to escalate conflict further.

The U.S. Administration released the new National Cyber Strategy in September 2018, which has been characterized as "more aggressive" than previous iterations.[24] Federal agencies are now authorized to conduct offensive cyber operations as part of a broader deterrence strategy. Cyber threats were identified as the top priority in the Director of National Intelligence's Global Threat Assessment of 2018. In addition, some argue that in the 2018 Nuclear Posture Review, the U.S. Administration has laid out a strategy of deterrence that could potentially be used in addressing cyberattacks:[25]

> The United States would only consider the employment of nuclear weapons in extreme circumstances to defend the vital interests of the United States, its allies, and partners. Extreme circumstances could include significant non-nuclear strategic attacks. Significant non-nuclear strategic attacks include, but are not limited to, attacks on the U.S., allied, or partner civilian population or infrastructure, and attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities.[26]

The United Kingdom recently released its National Cyber Security Strategy 2016-2021, which identifies cyberattacks as an issue of national security. The UK strategy established a new institution, the National Cyber Security Centre, which acts as the government's cybersecurity hub and as a nexus between government and private corporations. With its emphasis on defence, deterrence, and cybersecurity development, this effort has been lauded by some in the security community as a model for other states.[27]

The EU's collective cybersecurity strategy is centred around the EU Agency for Network and Information Security, which is mandated to support EU members states in the development and implementation of their individual national security strategies.[28] In addition to urging member states to develop their own cybersecurity plans, the EU is seeking to coordinate a policy for collective response to cyberattacks against its institutions. This was formalized in the creation of the Computer Emergency Response Team (CERT-EU) in 2017, whose mission statement includes responding to cyberattacks. The mission statement does not clarify how

responses will be conducted, though it does mention that CERT-EU will operate based on the value of ethical integrity.[29]

The North Atlantic Treaty Organization (NATO) established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in 2008. Based in Tallinn, Estonia, the CCDCOE marks NATO's acknowledgement that cyberspace is another frontier within which military campaigns are fought. It has published the Tallinn Manual 2.0 on how international law is applicable to cyberspace, and conducts military exercises such as Locked Shields, which simulates cyberattacks and integrates non-technical elements, effectively mimicking what a cyber war would look like.[30] The CCDCOE also hosts CyCon, which conducted its tenth edition in 2018. CyCon brings together technical, legal, policy, and military experts on cyber conflict issues, and its focus is on maximizing security in cyberspace.[31] In 2018, NATO also established its Cyber Operations Centre to coordinate and integrate member states' cyber capabilities into the rest of the Alliance's military strategies. These moves indicate NATO member states' perspectives on the severity of the threat posed by cyberattacks; despite framing the new Centre's creation around cyber defence,[32] some believe that it is more likely to be used as an offensive response mechanism in the event of a cyberattack. Rizwan Ali, who writes for Foreign Policy, states: "This is a marked departure from NATO's historical stance of using cyber only defensively, mainly to ward off incursions against its own networks. The more aggressive approach was intended as a strong message, primarily to Russia, that NATO intends to use the cyber capabilities of its members to deter attacks in the same way it uses land, sea, and air weaponry."[33]

The United Nations (UN), perhaps the best suited forum in which cyberattacks and conflict may be addressed by the international community as a whole, has made some progress towards a more cooperative approach. Issues of global governance are discussed in the UN, but there is little movement, likely because states are emerging as the key players in cyberspace. In 2004, the UN established the Group of Governmental Experts (GGE) to study and strengthen security in cyberspace at the global level. The GGE determined early on that international law does apply to cyberspace but has suffered setbacks in recent years due to disagreement among its 25 members on certain key issues, such as self-defence and the application of international humanitarian law.[34] It is unclear at this time whether the GGE will continue its work following the breakdown over these disagreements. Maurer and Taylor have outlined three potential paths forward. These include: a continuation of the GGE process with adjustments, such as opening the group up to all member states; a more

ambitious attempt at global cybersecurity governance such as Microsoft's proposal for a Digital Geneva Convention; or a narrowing of focus away from governance and towards bilateral (as opposed to multilateral) cybersecurity and economic cooperation.[35] While it appears that the UN has failed thus far to foster agreement at the international level, this is perhaps the perfect opportunity for the field of conflict resolution to influence the discussion.

Conflict resolution: cyberattacks and cyber conflict

In simple terms, the field of conflict resolution has greatly contributed to our understanding of how to address various types of conflict. In most cases, it is desirable to know the underlying grievances that conflicting actors harbour towards one another. Once those have been identified, any number of suggestions can be made that will meet the needs of the relevant parties, with the broader aim of eliminating the current conflict (negative peace) and transforming the relationship so that the possibility of future conflicts is minimized (positive peace).[36]

As conflict resolution has evolved, it has incorporated new approaches to conflict-producing situations. Ramsbotham labels the current iteration as a *cosmopolitan conflict resolution*, which is focused on the transnational nature of contemporary conflicts.[37] Transnational conflicts are characterized by global-local connectors including the flow of people, capital, ideas, weapons, and criminal networks, that bring global issues to the local, and local issues to the global.[38] Cosmopolitan conflict resolution aims to address the drivers of these conflicts, and to proactively promote conflict resolution values globally to mitigate violence before it occurs.

Practices such as mediation[39] and negotiation[40] have proven successful processes for managing and resolving conflict between individuals, groups, and even states, often with the intervention of a third party. Referred to by some as *interactive conflict resolution*,[41] these practices are contingent on the participation of representatives from each side. However, the problems posed by cyberattacks and cyber conflict pose a potential threat to these conflict resolution approaches, including cosmopolitan conflict resolution and interactive conflict resolution, one that has not yet been coherently addressed by the field.

The purpose of identifying the threat posed by such actions in cyberspace is not an exercise in fearmongering. Cyberattacks conducted by a mix of states and non-state actors, the risks posed by hybrid conflicts, and the movement into cyberspace of violent non-state actors

are realities, but they do not yet represent an inevitable future. Thus far, conflict resolution has advocated for the adoption of new technologies to augment traditional theory and practice, though it has been argued that the field has typically been slow to do so.[42] As such, this paper suggests that conflict resolution theorists and practitioners should focus more on what role their field can play in a new cyber landscape.

As we perceive it, there are two fronts that need to be addressed, corresponding (more or less) with practice and with theory. First, there is the inherently different nature posed by cyber conflicts as described in the preceding section. Of perhaps greatest import is the attribution problem – how do current conflict resolution tactics hold up when the perpetrator is unidentifiable or beyond the reach of conflict resolution advocates? At the very least the relationship between perpetrator and victim is highly asymmetrical, where the former wields almost all the power. To avoid becoming irrelevant as it relates to cyber conflict, mediation, negotiation and other conflict resolution models may need serious adjustments in this capacity. Some first input may be provided by literature on addressing cyberattacks by hackers such as Moty Cristal's article in *Wired* on negotiating with hackers.[43]

Secondly, and perhaps of a more urgent nature, is the need for conflict resolution to become engaged in the development of new technologies and discussions surrounding their governance at both the national and global level. Given the advantage of offensive strategies over defensive ones in responding to cyberattacks and cyber conflict, we argue that an emphasis should be placed on promoting conflict resolution values of peace and cooperation in the development of national cybersecurity strategies. This might include the training of technical engineers and software developers, similar to the scholar-entrepreneur-policy maker triad suggested by Miklian and Hoelscher,[44] as well as making policy suggestions to national governments and international organizations, such as the UN. The securitized response to terrorism following 9/11 and its consequences may provide an adequate analogy in this case. Conflict resolution should capitalize on this opportunity to insert itself in the cyberspace conversation early and loudly, rather than wait until unfortunate events take control away.

As Ramsbotham et al have noted, "technologies will transform the field of conflict resolution in ways that will make it unrecognizable to the founders and those who have worked in the field as academics and practitioners over the past fifty years."[45] Some fascinating work is

being done by various groups utilizing new communications technology, [46] which marks an important step for reconceptualizing conflict resolution practice.

Conclusion

In this paper, we have analysed the recent developments of cyberattacks and cyber conflict, which present new problems to be addressed by the field of conflict resolution. Some states have adopted a policy of coordination with non-state actors in the execution of cyberattacks. This corresponds with the emergence of hybrid wars in which cyberattacks are used alongside more conventional military tactics and involve a variety of state and non-state actors. Non-state actors also use cyberattacks in the pursuit of their own agendas, exemplified in the transition of ISIS from a quasi-state to a "cyber caliphate."

We have suggested that these developments are characterized by two key problems. Attribution of cyberattacks to a perpetrator is difficult because cyberspace allows such actors to operate anonymously and with no warning. In turn, this incentivizes offensive responses to pre-empt cyberattacks. States and international organizations are thus increasingly developing security strategies that identify cyberattacks as a significant threat. While some have sought a cooperative approach, others have used more aggressive language to deter would be attackers.

Given the development of securitized responses, we argue that the field of conflict resolution needs to become more engaged in the discussion surrounding cyberattacks and cyber conflict. To date, there has not yet been a coherent approach adopted by the field. Two fronts should be addressed. First is the adjustment of current conflict resolution models and the development of new models to adequately respond to the realities of cyber conflict. Second, the field needs to engage with technical experts and innovators, as well as policy formulators, to improve understanding of cyber conflict and instil conflict resolution values wherever possible. The model of researcher-entrepreneur-policy maker triad provides a good starting point.[47]

Some efforts have been made to incorporate new technologies in conflict resolution practice; however, these have mostly focused on mass mobilization and communication to promote a global peace agenda. This is, of course, commendable, but it does not address the ways in which cyberattacks and cyber conflict appear to be altering conflicts. We distinguish between the adoption of technology on one hand, and the addressing of

conflicts related to these developments on the other. Accomplishing the latter will no doubt involve re-conceptualizing conflict resolution theory, conducting research related to the implications of cyberattacks and the way in which they are being carried out, and the subsequent adjustment of conflict resolution practices.

Healy presents five possible futures of cyber conflict and cooperation, with the ideal future represented in his "paradise" model. His hypothesis envisages a future in which cyber defence is prioritized and cyber actors, including states, are constrained from threatening the stability of cyberspace.[48] If conflict resolution scholars and practitioners wish to support such a future, then they must address the threat of cyberattacks and cyber conflict today.

Notes

[1] Moty Cristal, How to negotiate when hackers are holding you to ransom, *Wired*, 15 May 2017. https://www.wired.co.uk/article/cyber-attacks-hackers-ransoms

[2] Oona Hathaway and Rebecca Crootof, The Law of Cyber-Attack, *Faculty Scholarship Series*, Paper 3852, 2012, p. 826. http://digitalcommons.law.yale.edu/fss_papers/3852

[3] Brandon Valeriano and Ryan Maness, The dynamics of cyber conflict between rival antagonists, 2001-11, *Journal of Peace Research*, vol. 51, iss. 3, 2014, p. 348.

[4] Thomas Rid attempts to reconcile the classical understanding of war with the addition of cyber elements, and determines that a cyber war would require, aside from an instrumental purpose and political motive, an element of (lethal) violence or force. Thomas Rid, Cyber War Will Not Take Place, *Journal of Strategic Studies*, vol.35, iss. 1, 5 October 2011, p. 29.

[5] See: Jon Lindsay, Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack, *Journal of Cybersecurity*, vol. 1, iss. 1, 2015.

[6] Ibid., p. 56.

[7] Scott Applegate, Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare, *IEEE Security and Privacy Magazine*, September 2011, p. 18.

[8] Ibid., p. 18.

[9] Ibid., p. 18.

[10] Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington, Virginia, 2007, p. 14.

[11]Andreas Jacobs and Guillaume Lasconjarias, NATO's Hybrid Flanks Handling Unconventional Warfare in the South and the East, *NATO Research Paper*, no. 112, Research Division – NATO Defence College, Rome, 20 April 2015, p. 2.

[12] Raymond Ridderhof, From Classic Wars to Hybrid Warfare, Blog, *Peace Palace Library*, 27 July 2017. https://www.peacepalacelibrary.nl/2017/07/from-classic-wars-to-hybrid-warfare/

[13] Kenneth Geers, Kosovo, Cybersecurity and Conflict Resolution, Conference paper, 2501 Research, 25 November 2014. http://www.2501research.com/new-blog/2014/11/25/kosovo-conflict-resolution

[14] For example, Estonia in 2007. See: Stephen Herzog, Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, *Journal of Strategic Security*, vol. 4, no. 2, Summer 2011, pp. 49-60.

[15] Rajeev Chaudrey, Violent Non-State Actors: Contours, Challenges and Consequences, *CLAWS Journal*, Winter 2013, p. 169.
[16] Christina Schori Liang, Dead or alive? The future of the Islamic State, Blog, *Global Insight*, Geneva Center for Security Policy, 2 May 2018. https://www.gcsp.ch/News-Knowledge/Global-insight/Dead-or-Alive-The-Future-of-the-Islamic-State
[17] Christina Schori Liang, Unveiling the "United Cyber Caliphate" and the Birth of the E-Terrorist, *Georgetown Journal of International Affairs*, vol. 18, no. 3, Fall 2017, p. 16.
[18] Martin Libicki, *Cyberdeterrence and Cyberwar*, The RAND Corporation, Santa Monica, 2009, p. 43.
[19] Hans-Georg Massen, Verfassungsschutz warnt vor Cyberangriffen, *Zeit Online*, 14 May 2018. https://www.zeit.de/politik/deutschland/2018-05/hans-georg-maassen-verfassungsschutz-cyberangriff-warnung
[20] Richard Andres quoted by Andrea Locatelli, The Offense/Defense Balance in Cyberspace, *Istituto Per Gli Studi Di Politica Internazionale Analysis* No. 203, October 2013, p. 8.
[21] Locatelli, p. 9.
[22] Global Cybersecurity Index, International Telecommunications Union, Date unknown. www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[23] Half of all countries aware but lacking national plan on cybersecurity, UN agency reports, *UN News*, 5 July 2017. https://news.un.org/en/story/2017/07/560922-half-all-countries-aware-lacking-national-plan-cybersecurity-un-agency-reports
[24] Ellen Nakashima, White House authorizes 'offensive cyber operations' to deter foreign adversaries, *The Washington Post*, 20 September 2018.
[25] Jeffrey Lewis, "WannaCry" about Trump's nuclear posture review? The global implications of deterring cyber attacks with nuclear weapons, Analysis, Nuclear Threat Initiative, 18 June 2018. https://www.nti.org/analysis/articles/wanna-cry-about-trumps-nuclear-posture-review/
[26] United States, Department of Defense, Office of the Secretary of Defense, *2018 Nuclear Posture Review*, February 2018. https://www.hsdl.org/?view&did=807875
[27] Danielle Kriz, A Global Model: UK's National Cyber Security Strategy, Paper, Security Roundtable, 9 May 2017. https://www.securityroundtable.org/global-model-uks-national-cyber-security-strategy/
[28] See: Annegret Bendiek, Raphael Bossong, and Matthias Schulze, The EU's Revised Cybersecurity Strategy Half-Hearted Progress on Far-Reaching Challenges, *SWP Comments*, no. 47, November 2017. https://www.swp-berlin.org/fileadmin/contents/products/comments/2017C47_bdk_etal.pdf
[29] CERT-EU, *RFC 2350 CERT-EU*, Computer Emergency Response Team, January 2018. https://cert.europa.eu/static/RFC2350/RFC2350.pdf
[30] NATO CDCOE, *2017 COE Catalogue*, NATO Cooperative Cyber Defence Centre of Excellence, December 2016. https://ccdcoe.org/sites/default/files/documents/COE%20CATALOGUE%202017.pdf
[31] NATO CDCOE, Cyber Security Conference/CyCon 2018, NATO Cooperative Cyber Defence Centre of Excellence, Date unknown. https://ccdcoe.org/cycon-2018.html
[32] Rachel Ansley, Here's Why NATO's Cyber Operations Center is a Big Deal, *New Atlanticist*, Atlantic Council, 9 November 2017. http://www.atlanticcouncil.org/blogs/new-atlanticist/here-s-why-nato-s-cyber-operations-center-is-a-big-deal
[33] Rizwan Ali, NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons, *Foreign Policy*, 7 December 2017. https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/
[34] Stefan Soesanto and Fosca D'Incau, The UN GGE is dead: Time to fall forward, *ECFR News*, 15 August 2017. https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance
[35] Tim Maurer and Kathryn Taylor, Outlook on International Cyber Norms: Three Avenues for Future Progress, Analysis, Just Security online forum, 2 March 2018. https://www.justsecurity.org/53329/outlook-international-cyber-norms-avenues-future-progress/

[36] Oliver Ramsbotham, Tom Woodhouse and Hugh Miall, *Contemporary Conflict Resolution* (4th ed.), Cambridge: Polity Press, 2016, p. 14.
[37] Ibid., p. 314.
[38] Ibid., pp. 121-123.
[39] Kenneth Kressel Chapter Thirty-Four: The Mediation of Conflict: Context, Cognition, and Practice, in Peter T. Coleman et al., *The Handbook of Conflict Resolution: Theory and Practice* (3rd ed.), Jossey-Bass, 2014, pp. 817–848.
[40] Roy Lewicki and Edward Tomlinson, Chapter Thirty-Three: Negotiation, in Peter T. Coleman et al., *The Handbook of Conflict Resolution: Theory and Practice* (3rd ed.), Jossey-Bass, 2014, pp. 795–816.
[41] See: Nadim N. Rouhana, Interactive Conflict Resolution: Issues in Theory, Methodology, and Evaluation, Paul C. Stern and Daniel Druckman, *International Conflict Resolution after the Cold War*, National Academy Press, 2000, pp. 294–337.
[42] Jason Gershowitz and Colin Rule, Applying Information and Communications Technology to Multiparty Conflict Resolution Processes, *ACResolution*, Fall 2012. http://colinrule.com/writing/acr2012.pdf
[43] Cristal, How to...
[44] Jason Miklian and Kristian Hoelscher, A new research approach for Peace Innovation, *Innovation and Development*, vol. 8, iss. 2, 2018, p. 193.
[45] Ramsbotham et al, p. 436.
[46] Games for Peace uses virtual worlds within popular games to facilitate interaction between adults and children from conflict regions. Currently only operating in Israel/Palestine, Games for Peace uses software to instantly translate chat messages from Hebrew, Arabic, and English to whatever language the listener speaks.
Games for Peace website: http://gamesforpeace.org/about-us/vision/
Perspective is a proprietary technology that uses artificial intelligence to rate a sentence or paragraph based on how it might be perceived by others, with the aim of reducing the use of toxic language to prevent the development of online echo-chambers. Users can test the potential impact that their posts may have online and adapt accordingly. Currently the software analyses conversations surrounding climate change, Brexit, and the US elections.
Perspective website, https://www.perspectiveapi.com/#/
Online Dispute Resolution has existed for some time, and makes use of online communication to both speed up dispute processes and to simultaneously require more thoughtful responses, since they must be typed rather than immediately articulated responses. Newer models seek to incorporate blockchain technology, currently popular for its use in cryptocurrencies like Bitcoin, to create incorruptible logs of dispute processes to ensure compliance.
Derric Yeoh, Is Online Dispute Resolution The Future of Alternative Dispute Resolution?, *Arbitration Blog*, 29 March 2018. http://arbitrationblog.kluwerarbitration.com/2018/03/29/online-dispute-resolution-future-alternative-dispute-resolution/
[47] Miklian and Hoelscher, p. 193.
[48] Jason Healy, The Five Futures of Cyber Conflict and Cooperation, *Georgetown Journal of International Affairs*, 2011, p. 115.