Bridging the Gap Between Cyber War and Cyber Peace

Introduction

'Cyber War is Coming!' So claimed John Arquilla and David Ronfeld in their seminal article in 1993.[1] 28 years later, it appears to have arrived. Cyberspace has been declared a new domain of warfare[2] and an increasing number of states are developing offensive cyber capabilities (OCC): human, technical, and virtual tools to destroy, disrupt and/or exploit the computer networks of an adversary for strategic advantage. There are an estimated sixty states with military or intelligence agency-based cyber units and twenty-nine of those possess declared OCC (as opposed to defensive cyber capabilities).[3] Although the use and development of cyber warfare capabilities often takes place under conditions of secrecy, and attributing cyber-attacks remains technically and legally problematic, the overall trend is unmistakable: a variety of international actors are now developing and using offensive cyber tools for a broad range of strategic uses, including espionage, subversion, coercion, war-fighting and for hybrid warfare campaigns.

As well as 'cyber war' becoming a growing reality and practice within military and intelligence establishments, a corresponding academic literature has emerged that has sought to conceptualise it, examine the strategic implications of cyber-attacks, and explore the ways in which they are being used to achieve military and political gains.[4] As with many areas of contemporary security studies, these approaches have been dominated by the realist and strategic studies approaches. The majority of the literature has been based on extending traditional and structural Cold War concepts to a new technology, and debates about deterrence, coercion, conflict escalation dynamics and security dilemmas have been a central focus.[5] While there has been a substantial body of work on cyber norms (responsible state

[1] Arquilla, John and David Ronfeldt, Cyberwar is Coming! Santa Monica, CA: RAND Corporation, 1993. https://www.rand.org/pubs/reprints/RP223.html.
[2] NATO CCDCOE (2017). "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit", available: https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html, accessed 09.09.18.
[3] Valentino-DeVries, J. and Yadron, D. (2015). "Cataloguing the World's Cyberforces", *Wall Street Journal*, available: https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710, accessed 19.02.18.
[4] See for example: Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5-32. Stone, John. "Cyber War Will Take Place." *Journal of Strategic Studies* 36, no. 1 (2013): 101-08..
[5] Ryan, N. (2018). Five Kinds of Cyber Deterrence. *Philosophy & Technology, 31*(3), 331-338.

behaviour),[6] and more limited literatures on confidence and capacity building,[7] the more fundamental debate about what constitutes cyber peace (and how to achieve it) has been, in relative terms, underdeveloped.

This article seeks to make a contribution to redressing this imbalance. We propose that cyber war is not just an empirical reality – something that states engage in - but an idea, metaphor, and narrative which needs challenging and deconstructing. In fact, cyber war has become an overwhelming pre-occupation in the cyber security discipline over the last two decades, which has structured, securitised and even militarised debates about cyber security in harmful ways. We also seek to operationalise existing peace and conflict studies, and desecuritisation concepts, to show how we might begin to shift the debate away from cyber war to a more academically grounded focus on cyber peace. To this end we suggest how we might begin to rearticulate the cybersecurity narrative and shift the debate away from securitization and cyberwar. It is argued that such a move away from a vicious circle where cyberspace is framed predominantly within a national security narrative and where states seek to perpetually prepare for cyberwar in the name of stability, to a virtual cycle of positive cyber peace, is both a desirable and necessary outcome going forward. We assert that this is particularly important if we are to avoid continuing to construct the very vulnerabilities and insecurities that lead to the prioritisation of offense and destruction, rather than transformative, human-centred ICT development.

The article is divided into three main sections to articulate its argument. The first explores the emergence of the term cyber warfare, the use of the concept to describe a broad range of cyber activities below the use of armed force, the conflation and confusion that has been caused by misuse of the term, and the harm caused by the securitization of cyberspace and the relentless pursuit of cyber warfare capabilities by national militaries and intelligence agencies. This section attempts to crystallise the shortcomings of the cyber war debate. The second section draws on securitisation theory as a means to explain the emergence of the cyber war narrative, and then unpacks the conceptual foundations of *de*securitisation, critically discussing potential pathways to desecuritisation in cyberspace in relation to existing language, practices and

[6] Grigsby, A. (2017). The End of Cyber Norms. *Survival, 59*(6), 109-122.
[7] Borghard, E., & Lonergan, S. (2018). Confidence Building Measures for the Cyber Domain. *Strategic Studies Quarterly, 12*(3), 10-49. Pawlak, P., & Barmpaliou, P. (2017). Politics of cybersecurity capacity building: Conundrum and opportunity. *Journal of Cyber Policy, 2*(1), 123-144.

processes. The final section charts a different course for cyber scholarship, policy and practices by outlining how peace building, conflict management, mediation and conflict prevention concepts can be used to further refocus the terminology and goals of the discipline and facilitate certain types of desecuritisation.

Cyberwar as idea, narrative, and metaphor

What is 'cyber war'? Providing a straightforward answer to that question continues to be problematic. War is traditionally understood as an extension of political disputes, involving uniformed combatants, the use of force to achieve political objectives, something that occurs within a defined geographical area, that incurs a certain number of battlefield casualties, is fought according to certain acceptable and commonly understood standards and rules, and which involves nation states. Modern cyber operations rarely fit these conventional parameters. There is also a degree of conflation and contestation in the academic literature. Perhaps most famously, Thomas Rid claimed that cyber warfare will not take place, because cyber-attacks are never at the same time political, lethal and instrumental.[8] Rid emphasised that the majority of activity fell below the threshold of the use force, and was better understood as subversion, sabotage or espionage. Other scholars have emphasised the force amplifier and multiplier effects of cyber warfare, arguing that cyber-attacks are supplements to military operations and are useful tools to achieve battlefield effects.[9] In this conception the use of cyber-attacks is often justified as a substitute for military force, or indeed for force protection – protecting militaries on deployment. A third conception of cyber warfare is that it is information warfare through the medium of cyberspace. According to this framing, cyber-attacks are used to disrupt, deny, degrade, manipulate and/or exploit the information stored on and carried by computer networks for strategic effects, including during hybrid warfare campaigns.[10] By this understanding cyber warfare is something that targets information as opposed to infrastructure, occurs outside of military conflict as often as in it, and has become an enduring and constant feature of contemporary international relations.

However cyber warfare is defined - and, just as with the term 'terrorism', there is unlikely to

[8] Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5-32
[9] Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly, 12*(3), 90-113.
[10] For a detailed discussion linking cyber warfare and information warfare concepts, see Ventre, D (ed.) (2011). Cyberwar and Information Warfare (Wiley Press).

be a uniform definition or understanding across polities - explanations for the emergence of cyber warfare as an empirical phenomenon are fairly limited. At the systemic level, a focus of structural realist accounts of international relations, cyber capabilities emerge to fulfil political needs within an anarchic system (and a global network of computers), which is ungoverned and ungovernable by nation states. In this sense, cyber war capabilities are developed as a natural extension of (and new medium for) existing geopolitical tensions and disputes. The development and use of cyber warfare capabilities by one power drives fear and uncertainty in other states, who invest in similar capabilities themselves. According to this logic, cyber warfare is a strategic chain reaction caused by security dilemmas. That these systemic dynamics are only now receiving sustained and rigorous academic attention,[11] and that the second order effects of cyber deployment (such as arms races) are only beginning to be fully recognised,[12] is surprising and disconcerting. A further explanation relates to the nature of the domain of cyberspace itself. Because cyber capabilities can be used covertly, and cyber-attacks are difficult to attribute (at least legally and politically, if not technically), they are attractive to revisionist actors, who use them as part of hybrid operations (in combinations with special forces operations, disinformation and propaganda, and economic or political coercion) to advance national interests.[13]

Most of these structural and systemic explanations of the emergence of cyber warfare fail to fully appreciate the historical, cultural and ideational drivers of cyber conflict and indeed the cultural, historical and political contexts in which cyber war capabilities have emerged. Cyber warfare entered the popular imagination during a period of immense historical change and uncertainty. In the 1990s, the fear of hackers, often depicted as cloaked and masked figures, began to displace the fear of the 'communist under the bed'.[14] The instability caused by the disintegration of states in the post-Cold War era and the emergence of complex identity-based conflict was also formative. In Kosovo, in 1999, networks of Serbian and Chinese hackers retaliated through cyberspace for the bombing of Serbian forces and the Chinese embassy. This

[11] Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701-715; Buchanan, B. (2017). *The cybersecurity dilemma: Hacking, trust and fear between nations*.

[12] Limnéll, J. (2016). The cyber arms race is accelerating - what are the consequences? *Journal of Cyber Policy*, *1*(1), 50-60.

[13] For further discussion of the role of cyber in contemporary hybrid warfare, see: Ducaru, S. (2016). The Cyber Dimension of Modern Hybrid Warfare And Its Relevance For Nato," *Europolity*, *10*(1), 1-17.

[14] Best, K. (2003). Revisiting the Y2K Bug: Language Wars Over Networking the Global Order. Television & New Media, 4(3), 297-319. Ross, A, "Strange Weather. Culture, Science, and Technology in the Age of Limits, 1991, Andrew Cass. P. 76

fed into concerns within national security establishments that the modern battlefield was no longer a place in which nations had the monopoly on the use of force, and that a form of warfare was emerging unlike what soldiers had faced before.[15] These dynamics were compounded by the Millennium (Y2K) Bug, an event which many feared would lead to a global internet meltdown, and which set a precedent for military involvement in cyber security affairs.[16] The war on terror perhaps did more than anything to heighten fears around the internet, with fears about cyber terrorism and 'cyber doom scenarios' (digital 9/11s) emerging out of acts of real violence by jihadists.[17] This period of fear and uncertainty corresponded with an exponential growth in internet users, the formation of social networks, and the use of securitising discourse to present the internet as something that need to be managed, controlled and fought over. As Richard Ashley has argued, the conditions of the post-Cold War era - particularly the uncertainty that was inherent in policymaking and academic communities during this period - created the conditions (a vacuum) for new security narratives (cyber war in this case) to emerge.[18] The cyber war narrative thus gave meaning and order to a seemingly anarchic international environment. Cyber war was not the only narrative that filled the gap created by the demise of the Soviet Union. Fears over environmental and social disintegration and the threat of civilisational conflict and jihadism were also prominent and the destabilising impact of technology on national and global security became a dominant discourse that was often integrated with other security concerns – the overwrought fear of cyber terrorism, for example.

Importantly, the emergence of cyber warfare has come to constitute an overarching narrative which has been disseminated by and proved beneficial to a variety of actors. In this sense, cyber war was not just an apolitical tool driven by uncertainty in the security environment, but a concept which has been deliberately constructed and connected to discourse, ideas and behaviours that have permeated, and served the interests of, a host of different security communities. These include the popular and social media, where cyber war is often depicted in apocalyptic terms - often for commercial reasons (click bait, as it is euphemistically known) - and in military establishments, which have tended to lean on conventional military strategic

[15] Borger, J. (1999). Pentagon kept the lid on cyberwar in Kosovo, The Guardian, https://www.theguardian.com/world/1999/nov/09/balkans, accessed 20 May 2020.
[16] Quigley, K. (2004). The Emperor's New Computers: Y2K (Re)Visited. *Public Administration*, 82(4), 801-829. Quiggin, J. (2005). The Y2K scare: Causes, Costs and Cures. *Australian Journal of Public Administration*, 64(3), 46-55.
[17] Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics*, 10(1), 86-103.
[18] Ashley R. (1995) The Powers of Anarchy: Theory, Sovereignty, and the Domestication of Global Life (1988). In: Der Derian J. (eds) *International Theory*. Palgrave Macmillan, London.

thought to attempt to grasp the implications of new technologies. As Alves has argued, the use of 'battlefield' analogies to frame cyberspace has contributed to the securitisation and militarisation of the internet and helped to dismiss the negative impacts of increasing state control and surveillance, while at the same time eroding trust, freedom and creativity.[19] Lawson takes a similar view, arguing that the cyber war discourse is indicative of "an ongoing crisis of effectively identifying and understanding what is old and new, the same and different about cyber conflict".[20] These cultural and discourse-based interpretations of cyber war exist not solely due to intellectual lag, but because of deliberately constructed narratives about the nature of cyber conflict cross a variety of communities that are interested in (and have interests in) cyber security being framed in this way. Cyber war narratives are thus *strategic* narratives - rhetorical devices to package and frame a security issue for strategic benefits. Scholars of IR have also benefited from these framings – creating fear can be used to justify the need for funded research on cyber security, and cyber hyperbole seeks and draws attention to analyses in popular media and other outlets.

The harms and shortcomings of the cyber war narrative have crystallised during this period. At the geopolitical level, the adoption, development and diffusion of cyber warfare capabilities, and the diffusion of certain ideas and characterisations about cyber war that justify their development and use, have led to destabilising practices among many of the world's leading cyber powers. The widespread global damage caused by the WannaCry virus, the continued reverse engineering and widespread diffusion of the Stuxnet malware, the use of cyber-attacks to destabilise political systems, as in the case of the 2016 US election, and the wholescale cyber espionage on the part of some states, all serve as examples. The emergence of 'cyber war' has heightened tensions between world powers, and contributed to the ongoing erosion of the rules-based international order. The latest offensive doctrines of the world's great powers, for example, suggest it is acceptable to 'defend forward' in cyberspace, and to continually and persistently engage your adversaries, regardless of conceptions of sovereignty[21]. In the Russian

[19] Alves, Artur de Matos (2015). Between the "Battlefield" Metaphor and Promises of Generativity: Contrasting Discourses on Cyberconflict *Canadian Journal of Communication* Vol 40 (2015) 389–405, p. 390.
[20] Lawson, S (2012). Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*, Volume 17, Number 7 - 2 July 2012, available: https://firstmonday.org/ojs/index.php/fm/article/download/3848/3270 doi:10.5210/fm.v17i7.3848
[21] For related discussions see: Healey, J., & Caudill, S. (2020). Success of Persistent Engagement in Cyberspace. *Strategic Studies Quarterly, 14*(1), 9-15. Smeets, M. (2020). US cyber strategy of persistent engagement & defend forward: Implications for the alliance and intelligence collection. *Intelligence and National Security, 35*(3), 444-453.

and Chinese cases, cyber-attacks have been used against power and energy grids, nuclear infrastructure, and other civilian infrastructure. Some cyber operations have been responded to with military force, as in the Israeli air strike against a Hamas hacker facility, and many of the world's leading powers' cyber doctrine is based on keeping force on the table as an option to respond to network-based attacks. While deterrence and restraint may be important factors in preventing the most damaging forms of attacks,[22] significant evidence has emerged that the world's leading powers are seeking to pre-emptively install malware into foreign critical infrastructure in the expectation of future conflicts.[23] Few scholars would argue that the current state of cyber security is anything but risky, dangerous, and harmful to international peace and stability, and increasing attention is being placed on the range of other harms caused by offensive cyber operations, including psychological, social/societal, economic, physical and digital harms.[24] The recent increase in attacks on health infrastructure and the exploitation of the Covid crisis by hackers to commit cybercrime is illustrative of the connections between wider social instability and cyber operations and the need for ongoing remedies that don't exacerbate the problems.

The shortcomings of the cyber war narrative and practice are evident in other areas of policy and intellectual debate too. Cyber warfare is often used to justify protecting the nation state, even when the protection of people or groups, including vulnerable communities, *within* the state is not fully considered. Cyber warfare has led to overly militarised approaches to cyber security and the involvement of the military (and intelligence agencies) in traditionally civilian areas of society, even when police, justice or crime-based approaches may be more suitable to countering cyber threats (in the same way that the 'war on terror' was an overly militarised approached to a transnational security threat). Often, military involvement is justified through the notions of the permanency and constancy of cyber war; as UK Chief of Staff General Sir

[22] Valeriano, B., & Maness, R. (2015). Theories of Cyber Conflict: Restraint, Regionalism, Espionage, and Cyber Terrorism in the Digital Era. In *Cyber War versus Cyber Realities* (p. Cyber War versus Cyber Realities, Chapter Chapter 3). Oxford University Press.
Taillat, S. (2019). Disrupt and restraint: The evolution of cyber conflict and the implications for collective security. *Contemporary Security Policy*, *40*(3), 368-381.
[23] Gjelten, T. (2013) Pentagon Goes On The Offensive Against Cyberattacks, available; https://www.npr.org/2013/02/11/171677247/pentagon-goes-on-the-offensive-against-cyber-attacks?t=1600499884941
[24] Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, David Upton, A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, *Journal of Cybersecurity*, Volume 4, Issue 1, 2018, tyy006, https://doi.org/10.1093/cybsec/tyy006

Nick Carter described it, we are "at war every day".[25] Despite this, cyberspace is not a controllable or conquerable territory and is fundamentally ill-suited to the logic of national, defendable boundaries.[26] As Lawson argues, the proliferation of these types of narratives leads to "the adoption of counterproductive, even dangerous policies".[27]

In the academic sphere, moreover, 'cyber war' has created a cottage industry of academic work focused on deterrence, the offence-defence balance, coercion and escalation. While this literature could tangentially claim to be related to peace (if peace is based on military strength, when deterrence creates stability, or because escalation need to be managed etc.) the attention to the intricacies of cyber *strategy* has created disciplinary path-dependencies and led to the neglect of other, more holistic approaches to the subject. To the detriment of a broader approaches to mitigating cyber insecurity, and as expected by securitisation scholarship, members of the field have "coalesced around a shared set of interests, common distinctive ways of generating knowledge (about threats, in the case of security) and shared strategies to tackle problems."[28]

From securitisation to desecuritisation: pathways to cyber peace (and their limitations)

How then do we move beyond the cyber war narrative to a more focused examination of cyber peace? This section of the article presents the argument that desecuritisation of the field is a necessary first step towards that goal, highlighting how and why cyber has been securitised, and the theoretical and practical steps that could be taken to reverse that process.

Securitisation as a concept emerged from work by the Copenhagen School group of scholars, most notably Barry Buzan and Ole Waever, in the early 1990s.[29] According to this particular school of thought,[30] securitisation is the process through which security issues emerge. Using

[25] Dominic Nicholls, "Britain is 'at war every day' due to constant cyber attacks, Chief of the Defence Staff says", The Daily Telegraph, September 29, 2019.
[26] Myriam Dunn Cavelty (2012), 'The Militarisation of Cyber Space: Why Less May Be Better', *4th International Conference on Cyber Conflict*, Tallinn, NATO CCD COE, p. 12.
[27] Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats, *Journal of Information Technology & Politics*, 10:1, 86-103. P. 86.
[28] Balzacq, T., Léonard, S. and Ruzicka, J. (2016) ''Securitization' revisited: theory and cases', *International Relations*, 30(4), pp. 494–531. P. 505.
[29] See in particular: Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers
[30] This section draws predominantly on the Copenhagen School conception of securitisation. We acknowledge there is some contestation in the literature on securitisation, and that there are other forms and types of

'speech acts' – i.e. securitising discourse – securitising actors seek to justify the need for 'special measures' to be introduced to counter 'existential threats' to the state, or other 'referent objects'. Central to the idea of securitisation - a concept which has been applied to a host of security issues, including terrorism, migration, and climate change - is the notion that it has utility to the securitising actor as it justifies the introduction of new legislation, new powers, or, for example, increases in funding. Cyber insecurity has often been presented as an existential threat, not only to the state (the digital pearl harbour discourse is a prominent one), for example, but also to the global financial system. Arguably, cyber security has been *over* securitised, resulting in the conceptual and policy concerns highlighted in the preceding section.

For change to occur of course, we must consider in more detail how existing securitised discourse and practice can be transformed. What are the processes of desecuritisation – at a conceptual and practical level - that can facilitate such a move, and how might this happen in the contemporary, conflicted cyberspace milieu and the ineffective processes of norm creation that exist?

First, if securitization is a process involving a speech act, then 'speech' (including 'intertextual' - oral, written and visual - framings) itself needs to be recognised and targeted for desecuritisation and deconstruction. A greater degree of precision is needed around the term cyber war and the range of malicious activity that falls below the threshold of the use of armed force, including conflict, espionage, subversion, coercion, and even deterrence. Policymakers and academics should avoid lazy categorizations of these distinctly different phenomena, the conflation between them, and be more precise when using them in both academic analyses and policymaking. The widespread use of the term 'cyber-attack' is similarly problematic. Much of the malicious activity online would be better characterised as intrusion, trespass, exploitation, or operations, rather than attacks, especially as the number of 'attacks' which lead to damage or destruction of computer systems is proportionally low. Similarly, the use of cyber war metaphors and language also needs to be deconstructed. Dark and shadowy language used

securitisation, most notably (a) the Foucauldian (Paris School) approach, which, simply put, deals more with the securitisation of society by governments as a means of social/political control, and (b) the Aberystwyth school, which focuses more on the concept of 'emancipation'. For further insights on these debates, see Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization' Revisited: Theory and Cases. *International Relations*, *30*(4), 494-531.

to depict cyberspace as a "gloomy underworld",[31] the use of biological threat metaphors such as infodemic, virus, and worm to describe cyber-attacks, the aforementioned construction of cyber doom scenarios (e.g. digital 9/11),[32] and the equation of cyber-attacks with weapons of mass destruction (disruption) all create fear that shapes policy in unhelpful ways.

The term 'cyber security' itself is also worth targeting for desecuritisation. Over the last two decades, it has become embedded in university departments, degree programmes, policy documents, and national cyber security strategies. But 'security' as a goal appears to be increasingly unattainable, especially in the fractured and globalised 21st century security environment. Cybersecurity is a good example of this condition - cyber-attacks are not likely to ever stop, especially as the design of the internet is fundamentally unconducive to security. Software development processes are also skewed towards the commercial availability of cybersecurity products and maintaining low costs in competitive markets, at the expense of security, trust and reliability.[33] In this context, to stop using the word security to describe cyber issues will be very difficult, even though the phrase presents a paradox and oxymoron.

What then would a positive and desecuritising discourse look like for cyber peace? The resilience concept provides one pathway forward which shifts the focus towards the recovery of computer systems, but, in the cyber sphere, it is a term that is not widely understood, and which has myriad definitions. It has also been criticised as being part of securitisation processes themselves[34] and a product of contemporary neoliberalism.[35] Replacing offence and war with human rights discourses might be a more effective and powerful way of framing cybersecurity issues which could form the basis of a transformative political and policy agenda. This would include emphasising the effects cyber-attacks have on human rights, including freedom of speech and privacy, and the metaphors of war could be replaced by terms that have been used to frame peace movements, including justice, equality, compassion, mediation,

[31] James Shires (2020) Cyber-noir: Cybersecurity and popular culture, Contemporary Security Policy, 41:1, 82-107, DOI: 10.1080/13523260.2019.1670006 p. 82
[32] Sean Lawson (2013) Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats, Journal of Information Technology & Politics, 10:1, 86-103.
[33] Ko, RKL (2020). Cyber autonomy Automating the hacker – self-healing, self-adaptive, automatic cyber defense systems and their impact on industry, society, and national security, in Steff R, Burton J, Soare R (eds.) Emerging Technologies and International Security: Machines, the State, and War (Routledge).
[34] Philippe Bourbeau & Juha A. Vuori (2015) Security, resilience and desecuritization: multidirectional moves and dynamics, *Critical Studies on Security*, 3:3, 253-268
[35] Bourbeau, Philippe, & Ryan, Caitlin. (2017). Resilience, resistance, infrapolitics and enmeshment. *European Journal of International Relations, 24*(1), 221-239.

reconciliation, and non-violence. These terms have barely been applied to cybersecurity but could form a powerful collective discourse to animate future scholarly work and policy efforts. Similarly, if biological metaphors are used, emphasis on the sustainability of internet networks, healthy ecosystems, internet ecology, cyber hygiene and safety, are all more positive framings.

A more fundamental consideration is whether desecuritisation is normatively or politically desirable. Cyber securitisation has happened for a reason: to generate a sense of urgency around what has been perceived as an urgent problem, which needs extra resources and attention. If cybersecurity had not been securitised, the logic goes, the necessary measures would not have been taken to enhance security, and malicious actors would have taken advantage of an even faster expanding range of vulnerabilities. But this is a false logic for several reasons. First, it doesn't count the negative effects of securitisation processes, which in the cyber sphere involves: the militarization of security – a form of hyper securitisation[36]; the centralisation and nationalisation of cyber security strategies, which have not been a good fit for asymmetric network-based threats; and the creation of security dilemmas – where defensive measures are perceived by other actors as offensive. One way to desecuritise is to keep issues out of the security realm to begin with. This form of pre-emptive securitisation[37] could be started from now on, especially as a range of technologies, such as AI, 5G, Quantum, and IoT are set to create new cyber vulnerabilities. While keeping *cyber* from being securitised is not possible, a less polemic, hyperbolic debate on new and emerging technologies could be pursued. This pre-emptive approach to de/re-securitization would also align with conflict prevention techniques and principles, which have long been a part of peace and conflict studies approaches.

Of course, such processes are likely to be politically contested by the actors that have been responsible for securitisation in the first place, including militaries, media, industry and academia..[38] De-securitising actors might be found in the non-governmental and societal sector, which aren't as enmeshed in a military cyber industrial complex (e.g. in health, transport, energy, finance), but giving 'society' more responsibility for desecuritisation will not be easy. Societies are not independent actors, they do not have legal or regularity authority, and their

[36] Andreas Behnke NATO's Security Discourse after the Cold War: Representing the West, p. 186
[37] Bourbeau, Philippe, and Juha A Vuori. "Security, Resilience and Desecuritization: Multidirectional Moves and Dynamics." *Critical Studies on Security* 3, no. 3 (2015): 253-68.
[38] Hansen, L. (2012). Reconstructing desecuritisation: The normative-political in the Copenhagen School and directions for how to apply it. *Review of International Studies, 38*(3), 525-546.

impact in shaping cyber strategy is weak at present. There is also the possibility of cheating and/or divergence, where some actors use desecuritising moves while others don't, and the likelihood of divergence between forms and levels of cyber desecuritisation across democratic and non-democratic states.

Stabilisation, replacement, rearticulation, and silencing

Imagining what a desecuritised process for cyber might look like, beyond a change in discourse, and how it could be measured, is also worth exploring here. Recent scholarship has shed light on the multidirectional processes involved in desecuritisation that could be applied to cybersecurity issues. Perhaps the most detailed investigation of these questions is provided by Lene Hansen. Hansen argues that moving beyond the 'friend enemy' dichotomy that drives contemporary security debates, and which she argues is at the heart of securitization discourses, could involve four distinct processes. The first involves *stabilisation* – this of course is something already on the agenda of international cyber policy, especially through processes such as the Global Commission for Cyber Stability. In the conventional realm, such a process involves less violence, less militarism, and positive engagement, although there will be differing interpretations of what constitutes positive engagement and cyber peace. To draw on Hansen's own historical parallel, détente in the 1970s was undermined by the Soviet invasion of Afghanistan in 1979. Aggressive moves in cyberspace (e.g. Stuxnet, the attacks against Estonia in 2007, and WannaCry, for example) are similarly likely to undermine the move towards a more stable cyberspace. As further discussed in the next section, stabilisation is concomitant with negative peace and the absence of conflict in cyberspace, but less conducive to positive peace and the elimination of structural violence.

A second desecuritising process involves *replacement* – where cyber securitization would be replaced by the securitization of other political issues. In this sense, as discussed in the previous section, cybersecurity concerns have displaced the existential angst of the Cold War period and the hyper-securitized urgency of the war on terror. At the ideational level, as Behnke argues, 'At some point, certain 'threats' might no longer exercise our minds and imaginations sufficiently and are replaced with more powerful and stirring imageries'.[39] But that leads to the question, what would replace cyber securitization? And is it ethically desirable to create or

[39] Quoted in Hansen, ibid, p. 541.

acquiesce to new securitizing moves in other policy areas? Replacement of cyber securitisation processes will also be problematic because cyber technologies are not at an advanced stage of maturity and are constantly evolving. This temporal aspect of securitization is difficult to overcome in cyber, as opposed to other areas of international activity, such as post-war conflict settlement processes, where there has been a definitive end to conflict. Cybersecurity is interwoven with so many other security sectors to the extent that replacement is not likely to be a viable option.

A third option for cyber desecuritisation is *rearticulation*, which involves moving the issue (cyber) from the securitized space by "actively offering a political solution to the threats, dangers and grievances in question".[40] Such a move is more ambitious, involves a more fundamental resolution of political disputes, major shifts in the public sphere, a move beyond friend-enemy distinctions, changes in identity, and in the interests of cyber security actors. Efforts to rearticulate cyber conflict are likely to be resisted, however, especially by states who view cyber-attacks as an extension of strategies to assert and protect their national interests. Despite these obvious shortcomings, desecuritisation through rearticulation is more in line with the positive versions of cyber peace outlined and discussed further in the next section and could be worked towards incrementally.

Fourth, cyber desecuritisation could be achieved through a process of *silencing*, which is when an issue disappears or fails to register in security discourse. This might entail the active exclusion of cyber from security discourse, which is in line with the discursive change outlined above. Silencing the rhetoric of cyber war and attacks could be an active political agenda for those that recognise the risk and dangers of cyber securitization and be viable across a longer-term time horizon *resulting* from rearticulation processes. Some forms of silencing could involve the assimilation of discourse into another through establishing rules of representation, rather than its abolition.[41] In the cyber sphere, this might involve adapting the language in national cyber security strategies, for example. Another way to silence cyber war narratives is to confront them and adapt them through institutional mechanisms and/or social movements – this could involve civil society and societal actors challenging the narratives constructed by security agencies. The inherent peril here is whether silencing can be achieved without

[40] Hansen, ibid, p. 542.
[41] Theismeyer, LJ (ed.) (2003). Discourse and Silencing: Representation and the Language of Displacement (John Benjamins Publishing Company) p. 13.

exacerbating tensions over freedom of speech and expression. A process of desecuritisation through silencing could lead to the oppressive and anti-democratic practices it was meant to replace.

Conflict Resolution and Peace Studies: Contributing to Desecuritisation

Moving beyond desecuritising moves, the question becomes, what would cyber peace look like and what would be its core characteristics? To answer these questions, this section of the article explores some of the conditions on which cyber peace could be based and how existing practices, particularly those surrounding peace building, conflict management, mediation and conflict prevention, could be used to refocus the terminology and goals of the discipline.

It should be noted from the outset that cyber scholars and policy makers are not disinterested in cyber peace. The norms debate in cyber security scholarship has certainly been a prominent one,[42] and a community of international cyber law scholars have conducted thorough investigations of how the existing laws of armed conflict apply to cyber warfare debates and issues.[43] There are also a variety of new think tanks, NGOs, policy institutes and industry initiatives dedicated to the peaceful use of cyberspace, including, among others, the Cyber Peace Alliance, Cyber Peace Institute, The Hague programme for cyber norms, the Global Commission for Cyber Stability (GCCS), the Cybersecurity Tech Accord and ICT4Peace. Moreover, state-led international, multi-stakeholder initiatives such as the Paris Call for Trust and Security in Cyberspace have outlined key principles on which the scope and meaning of cyber peace could be based.[44]

While this bodes well for normative and positive progress on cyber security issues, the academic and conceptual debate about cyber peace itself, what it looks like, and how it might be achieved, has not been subject to the same level of scrutiny. Indeed, whilst there is an emerging literature that frames the debate on cyberspace stability in terms of the achievement

[42] See, for example: Martha Finnemore and Duncan B. Hollis, (2016) 'Constructing Norms for Global Cybersecurity', The American Journal of International Law, 110 (3), July 2016, pp. 425-479
[43] Michael N. Schmitt (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge/New York: Cambridge University Press; Michael N. Schmitt (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge/New York: Cambridge University Press.
[44] Shackleton, Scott (2019), In a World of Cyber Threats, the Push for Cyber Peace is Growing, *The Conversation*, 3 September 2019, https://theconversation.com/in-a-world-of-cyber-threats-the-push-for-cyber-peace-is-growing-119419 accessed 23.06.20

of peace, major questions are in need of further exploration, in particular relating to how the core concepts from peace and conflict studies can guide and inform further analysis in the context of the rearticulation-desecuritisation pathway, which we regard as the most viable in the existing cyber milieu.

What makes it difficult to pin down how to achieve and indeed conceptualise cyber peace is the lack of consensus in the literature on what this means.[45] For some, it means deterrence and the absence of conflict and direct violence, or *negative peace*. For others, negative peace 'fails to address the primary sources of adversarial cyber operations today…espionage, (social) media influence, economic coercion and political intervention' that fall below the threshold of an act of aggression, threat or use of force or armed attack stipulated in the UN Charter. This, it is argued, provides aggressors with modes of operation that do not contravene existing international law but which clearly contradict the spirit of it. The consequence is that rearticulation and movement to positive cyber peace is clearly impeded.[46] From this perspective, positive cyber peace implies something more transformative, with the absence of disorder, disturbance and structural violence underpinning a collective form of security for cyberspace. To this end, the arguments for positive cyber peace, which we suggest are helpful for a strategy of rearticulation (and potential silencing in the long term), have centred on sustainable development, human rights, human security[47] and polycentric governance[48] as vehicles for facilitating a movement away from a focus on the state and war to ensuring security for individuals in cyberspace. Moreover, as an extension to this, scholars have focused on how capacity building, development and economic growth and symmetry can lead to a state of positive rather than negative cyber peace, through building sustainable prosperity, resilience and security. Furthermore, the limited work on how the conflict studies literature can be usefully applied to cyberspace has highlighted how and when third party mediation, negotiation

[45] Shackleton, Scott (2013) The Meaning of Cyber Peace, Institute for Advanced Study, University of Notre Dame https://ndias.nd.edu/news-publications/ndias-quarterly/the-meaning-of-cyber-peace/
[46] Kanuck, Sean (2019) Promoting Peace and Stability in Cyberspace in Cecelia M. Bailliet (ed) (2019) *Research Handbook on International Law and Peace*, Edward Elgar, 477-492
[47] Ibid; Roff, Heather. M. (2016) Cyberpeace: Cybersecurity Through the Lens of Positive Peace, New America, Cybersecurity Initiative, March 2016. References to human security in this article are used to denote a move from a focus on the state and a national securitised approach to a focus on the individual for the purposes of desecuritisation and transformation. To this end, whilst human security is important in relation to a focus on the individual, a human-centric approach also puts emphasis on user participation in the decentralised governance of cyberspace for the purpose of achieving positive cyber peace dynamics. For more on this argument in relation to desecuritisation and the actors involved in it beyond the state, see: Burton, J., & Lain, C. (2020). Desecuritising cybersecurity: towards a societal approach. *Journal of Cyber Policy*, 5(3), 449-470.
[48] Shackleton (2013), op.cit.

and intervention might be applied to prevention and in response to cyber conflict and cyber-attacks.[49] Others have focused on preventative diplomacy, mediation and regional solutions to reduce cyber conflict and subsequently build trust and peace in cyberspace.[50]

How then, can the concept of cyber peace and a human-centric approach (security and rights) be operationalised to facilitate rearticulation and bring about a better understanding of the process of cyber peace and how it can be realised? What can the tools available to those in the conflict resolution field contribute to such a process and what are the limitations?

Certain authors posit that this must be done through addressing the technological and the informational dimensions of cyber peace, whilst acknowledging that current trends mitigate against achieving even a negative cyber peace. From a technological perspective such trends include the exponential growth in ICT innovation, the increase in the number of states that are developing cyber offensive rather than defensive capabilities,[51] and the asymmetric incentive structure to conduct cyber-attacks and/or espionage. Such trends have continued despite initiatives to build confidence, reduce risk and come to some broad consensual agreement between states on norms to guide behaviour in cyberspace.[52] At the UN level, for example, the most prominent process has been that of the Group of Governmental Experts (GGE), which reached a consensus report on eleven norms of state behaviour in June 2021.[53] But whilst the UNGGE platform has meant that the Confidence Building Measures (CBMs)[54] – such as transparency and certain information sharing platforms – have been put in place and extended through the Organisation for Security and Cooperation in Europe (OSCE) process, as well as being reinforced by bilateral CBMs between China and other countries (e.g. the US, UK, Australia, Canada) and within multilateral fora on cyber espionage (G7 and G20) - there exist

[49] Valeriano, Brandon and Maness, Ryan C. (2018) The Dynamics of Cyber Dispute Mediation and Resolution, https://www.researchgate.net/publication/326926198_The_Dynamics_of_Cyber_Dispute_Mediation_and_Resolution accessed 23.06.20; Wohlfield, Monika and Jasper, Jack (2018), Cyberattacks and Cyber Conflict: Where is Conflict Resolution?, https://www.um.edu.mt/library/oar/bitstream/123456789/38298/1/Cyberattacks_and_Cyber_Conflict_Where_is_%20conflict_resolution_2018.pdf accessed 23.06.20

[50] Pawlak, P., Tikk, E. & Kerttunen, M. (2020) Cyber Conflict Uncoded: The EU and Conflict Prevention in Cyberspace, https://www.iss.europa.eu/content/cyber-conflict-uncoded accessed 23.06.20

[51] Kanuck, op.cit.;

[52] Confidence building and norms processes have been widespread, including at the UN, OSCE and through various bilateral agreements

[53] Solomon, H. (2021). UN report could be 'positive step' in establishing nation-state cyberspace norms, says Canadian expert, available: https://www.itworldcanada.com/article/un-report-could-be-positive-step-in-establishing-nation-state-cyberspace-norms-says-canadian-expert/454182, accessed 8 June 2021.

[54] Hitchens, Theresa and Gallagher, Nancy W. 'Building confidence in the cybersphere: a path to multilateral progress', *Journal of Cyber Policy*, 4 (1), 4-21

different interpretations of what this means in practice; violations of previous agreements have continued with subsequent unilateral action against aggressors, but with only limited effectiveness.[55]

Differences in the political interpretation of the norms required to govern state behaviour in cyberspace between cyber-sovereign and liberal-minded states has led to institutionalisation of such difference through competing processes at UN level.[56] The Open Ended Working Group (OEWG) proposed by Russia in 2018 now operates in parallel to the GGE deliberative process; it is difficult to see how such diplomacy can lead to a consensus that will be adhered to and which will lead to a situation of even negative cyber peace emerging. Whilst other multilateral and bilateral efforts have been evident that aim to facilitate the prevention and mitigation of conflict in cyberspace the challenge of overcoming competing approaches and legal interpretations of what is acceptable and not acceptable state behaviour in cyberspace is difficult to overcome, even when diplomats have promoted and secured broad normative agreements on key principles. Multistakeholder fora such as the GCSC or the Paris call, similarly, whilst providing voice to key stakeholders - which is important given the dual-use nature of ICTs – have not curbed, and do not seem that they will change in the near future the efforts of those states that seek to strategically enhance their cyber offensive capabilities. Whereas some scholars suggest certain problems and issues that plague the cyber norms processes identified can be remedied[57] to achieve at least a state of negative peace, others argue positive peace could be attained through a *pax informatica* approach,[58] through polycentric governance[59] and through rethinking cybersecurity in terms of the concepts of positive peace[60] and a human-centric approach.[61]

---

[55] Jakob Bund and Patryk Pawlak (2017) Minilateralism and Norms in Cyberspace, Issue Alert, EU Institute for Security Studies, 27 September 2017.

[56] To elaborate, those with a liberal approach led by the United States advocate for a multi-stakeholder model of governance, the applicability of existing international law to cyberspace, and a global, open, free and secure Internet that is accessible to all; and those with a 'national cyber sovereignty' approach – China, Russia, Iran and others in the Shanghai Cooperation Organization (SCO) – call for an intergovernmental governance model and advocate for state control of Internet content and architecture in order to maintain regime stability and protect national security interests.

[57] Christian Ruhl, Duncan Hollis, Wyatt Hoffmann and Tim Maurer (2020), Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads', Carnegie Endowment for International Peace, Paper, 26 February 2020

[58] Kanuck, op.cit.

[59] Shackleton, Scott (2014), *Managing Cyber Attacks in International Law, Business and Relations: Towards a Cyber Peace*, Cambridge/New York: Cambridge University Press

[60] Galtung, J. (1969) 'Violence, Peace and Peace Research', Journal of Peace Research, 6 (3), 167-191

[61] Roff, op.cit.; see also Reinhold, Thomas and Reuter, Christian (2019) From Cyber War to Cyber Peace, in Christian Reuter, *Information Technology for Peace and Security*, Springer, p139-164

These suggested approaches are not disconnected, of course. Underpinning the *pax informatica* approach is a rearticulation of security at the level of humanitarian need and benefit, in order to (re) frame the conversation 'around the socio-economic value of information and promoting cooperation'. In this way, it is argued we can achieve elements of positive peace. More precisely, it is argued that such an approach, that focuses on opportunities that ICT can offer, avoids the limitation of the *pax technologica* approach in the UN GGE process which is underpinned by a focus on the state and national geopolitical interests. Moreover, such an approach, through promoting human welfare, human development and the values of equality, social justice and non-discrimination in relation to the opportunities presented by ICT innovation can serve as better platform for delivering stability and positive peace. For example, CyFy Conferences such as CyFy India or CyFy Africa that focus on technology, security and society or established international covenants that secure fundamental 'rights' are upheld in relation to ICTs[62]. This does not imply that negative peace will not exist in parallel, but that it will exist in a context that at least offers relative stability and certainty in relation to the availability of future mechanisms and conduits for information flow, human security and peace. The advantages of such an approach – which is grounded in existing practice - is that it can promote international cooperation and capacity building in cyberspace which will not only bring benefits for peace in cyberspace but also more broadly.[63] The limitation is that whilst such an approach can indeed remove structural impediments to peace and address common development challenges, there is no guarantee that such information stability will or can transform the zero-sum games within the *pax technologica* approach (just as it has not done so, for example, beyond cyberspace). The question then becomes, of course, that of if and how the benefits of *pax informatica* can incentivise states to rearticulate their own narratives and converge through international law on viable rules of the road for their peaceful behaviour in cyberspace in order to create the right conditions for a sustainable cyber peace.

Further arguments in relation to human security and positive peace are also predicated on reimagining and rearticulating cybersecurity from a focus on the state as referent object, to the individual and/or societal groups. Moreover, the argument here is that framing the problem as one of cyber insecurity and negative peace (the absence of cyber-attacks) does not move us

[62] Kanuck, op.cit, 488-489.
[63] Kanuck, op.cit, 485-491.

away from the zero-sum games summarised above in relation to the *pax technologica* approach. Cybersecurity inevitably becomes the responsibility of the state, where the more cybersecurity is sought the more insecure cyberspace and the real world becomes. As Dunn Cavelty puts it, 'measures taken by some nations are seen by others as covert signs of aggression…and will likely fuel more efforts to master "cyber weapons" worldwide.'[64] We are therefore caught in a vicious circle within this framing where states seek to perpetually prepare for cyberwar, and where perceived relative gains in security represent an absolute loss to the cyberspace ecosystem.

Shifting the referent object – people and polycentric governance

This is the context in which a rearticulation and reframing is necessary in relation to the referent object of security, away from the state to the individual through a human-centric perspective and away from the notion of negative peace to positive peace. Both of these moves are necessary, it is argued, to first, capture a more nuanced notion of what constitutes violence in cyber war beyond the physical and lethal, to include a broader understanding of the dimensions of violence (psychological vs physical, object oriented, negative vs positive influence, direct/personal vs indirect/structural, intended vs unintended, potential vs latent[65]) that can be done to individuals through cyber means; and second, put the human at the centre of efforts so that any attempts by states to defend against cyber threats are underpinned by a rights-based framework to achieve cyber peace.[66] Putting the human front and centre of security considerations then, allows a bottom-up approach that builds connections outwards to other objects of security and how they connect to people; thus not limiting any benefits to the few or already powerful entities that might come from an emphasis on technology or infrastructure, for instance.

Such an approach culminates in a more fluid, layered conceptualisation of cybersecurity, with cyber insecurity and cyberwar at one end, and a state of (positive) cyber peace at the other. Through focusing on the individual and the relationship between interpersonal and structural violence discussed by Galtung, such an approach suggests a re-examination of 'the structure

[64] Dunn Cavelty, Miriam (2014), 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities', Science Engineering and Ethics, 20, 701-715;
[65] Galtung, op.cit.
[66] Roff, op.cit, p.6-7; Dunn Cavelty, op.cit. p707.

of cyberspace, the types of violence that occur within and through cyberspace,'[67] and how identified problems can be dealt with at source. Moreover, by conceiving the cyber ecosystem through a series of layers - physical, syntactic and semantic[68] - and human (and non-human) agents,[69] and placing the individual at the centre of the analysis, cybersecurity is conceptualised as a practice whereby humans can act *through* and non-humans can act *in* cyberspace. Such a conception, in turn, captures the horizontal and vertical dimensions of the cyber landscape where 'each structure, agent and content has meaning and is vulnerable in some way, and each must be secured through different means.'[70] Thus, for example, securing the content layer might involve stronger encryption (such as in the Hypertext Transfer Protocol Secure (HTTPS)) or indeed legislation that protects and allows individual control of personal data (for example, the EU's GDPR), securing the physical layer might involve a bilateral or multilateral non-interference agreement in relation to banning tapping into fibre optic cables or installing malware; and securing the syntactic layer, could be achieved through more secure protocols (for example, the Transport Layer Security (TLS) Protocol 1.3 developed by the IETF) or indeed more robust security of supply policies and initiatives to ensure that there are no backdoors to exploit in software (see, as one example, the Trustworthy Software Initiative sponsored by the UK government).[71]

The question that arises from the above bottom-up, positive peace and human-centred reconceptualization of cybersecurity is the type of governance that it lends itself to, in particular given that it is often states that seek to frustrate the emergence of secure hardware and software for the national security interest. Certain scholars have argued that a polycentric governance (similar to that in climate change) that embraces self-regulation and bottom-up initiatives is

[67] Roff, op.cit, p15

[68] Libicki, Martin (2009) Cyberdeterrence and Cyberwar, Santa Monica: RAND. The physical layer consists of physical infrastructure (cables, satellites etc.,), the syntactic layer of software and protocols and the semantic layer of information that translates code to normal language (content).

[69] Benkler (1998, 2007) makes a similar distinction between a physical layer (hardware), a 'logic layer' (software and protocols) and a social layer (culture, human contact, ideas and policy). Benkler, Y. (1998) 'The Commons as a Neglected Factor of Information Policy', www.benkler.org/commons.pdf, accessed 25 June 2020.
Benkler, Y. (2007), 'The Battle over the Institutional Ecology of the Digital Environment', http://cyber.law.harvard.edu/wealth_of_networks/11._The_Battle_Over_the_Institutional_Ecology_of_the_Digital_Environment, accessed 25 June 2020)

[70] Roff, op.cit. p12-13

[71] For a discussion of the debates on security related to a range of Internet protocols, see Harcourt, Alison, Christou George and Simpson, Seamus (2020), *Global Standard Setting in Internet Governance*, Oxford: Oxford University Press; see also DeNardis, Laura (2015) 'The Internet design tension between surveillance and security', IEEE Annals of the History of Computing 37 (2): April–June, 72–83; DeNardis, Laura (2009) *Protocol Politics: The Globalization of Internet Governance*. Boston, MA: MIT Press.

most suited to managing the Internet and achieving cyber peace[72]. Such an approach is premised on a multi-type, multi-sectoral, multi-stakeholder, multi-level, and multi-purpose model that places emphasis on diverse organisations working together to create policies that promote and increase levels of cooperation and compliance, and that enhance (cyber) regimes and flexibility. The argument for a polycentric approach also rests on a critique of top-down governance and the ability of singular governments to propose and implement solutions to complex collective problems and achieve cyber peace (for example, a singular Treaty for Cyber Peace). Polycentric governance, it is argued, can lead to more innovative practices 'developed organically from diverse ethical and legal cultures.'[73] This said, there are also several criticisms of such an approach to cyberspace and achieving cyber peace. First, that such an approach makes assumptions about certain features that are necessary for its success which are not obviously present in cyberspace, including that of a 'bounded community…identifiable and measurable resource scarcity and individual need, and the power of existing societal norms'[74]. Second, and related to this, is the assumption that a society must exist within existing norms of behaviour within the group and that such norms should be reinforced consistently by interpersonal interaction. In-group learning and adaptation, therefore, play a central role in changing and shaping behaviour. The prevalence of anonymity, and face-less interaction in cyberspace then, would constrain the logic of any such approach to norm formation, diffusion and implementation[75].

This is not to say that certain elements of the top-down or indeed the polycentric approach are not useful, but rather that they are not sufficient if we are to move away from cybersecurity narrative and governance framework whereby the state, and international laws made by states, are able to simply reinforce the right to self-defence (war) in cyberspace. To this end, it has been suggested that we can borrow fruitfully from existing evidence and literatures that have pointed to ways in which conflict can be resolved, and certain conditions and factors that are required to move to negative and positive peace. In terms of the latter, the Global Peace Index identifies several factors that are important for peace to be achieved: a sense of a collective group or society within which one interacts and a sense of where boundaries lay and overlap;

[72] Shackleton (2014), op.cit.
[73] Shackleton (2013), op.cit.
[74] Roff, op.cit. p6
[75] Roff, Ibid.

trust and how this can be fostered in relation to cyberspace;[76]and governance that must be socially just, rights-based, equitable and fair and where information is accessible and free flowing. Indeed, scholars working on cybersecurity suggest that 'to create a peaceful cyberspace [positive peace], the current debates need to go beyond the focus on norms, international law and confidence building measures…and include…the respect for human rights and fundamental freedoms, mechanisms for an effective fight against cybercrime…and creating a culture of cybersecurity.'[77]

Security and peace - practices and methods

We can thus ask how far the literature on peacebuilding and conflict resolution can provide us with the tools to inform the discussion in the direction of rearticulation and reaching positive cyber peace. How can the right conditions be created that will cultivate the emergence of factors that can lead to positive rather than negative cyber peace? More specifically, how can we move from distrust to trust in cyberspace across the different layers and agents involved, from heterogeneous to a collective cyber community(ies), from unequitable to equitable governance and information flow and provision? Certain scholars have argued that, given the impasse and failures within current diplomacy and CBM initiatives within the cybersecurity space, there is room to consider how other conventional conflict prevention and resolution methods can be operationalised in efforts to move to a 'culture of cybersecurity' that enables the achievement of cyber peace. Here preventative diplomacy,[78] part of a broader interactive conflict resolution approach,[79] which is non-coercive and non-escalatory, and can take many forms from mediation and early warning to adjudication and arbitration, can play a role in building trust between agents. In terms of early warning, for example, and addressing issues in the physical layer, enhanced monitoring and tracking mechanisms can highlight movement of offensive cyber systems, hardware and software, with a view to making involved agents more

[76] See also in relation to cyber peace: Inversini R. (2020) Cyber Peace: And How It Can Be Achieved. In: Christen M., Gordijn B., Loi M. (eds) *The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology*, vol 21. Springer, Cham, p.259-276

[77] Positive Peace in Cyberspace Workshop, EU Cyber Direct, https://eucyberdirect.eu

[78] See Boutros-Ghali, Boutros. "An Agenda for Peace: Preventive diplomacy, peacemaking and peace-keeping." *International Relations* 11.3 (1992): 201-218.

[79] Wohlfeld, Monika, & Jasper, Jack (2018). Cyberattacks and cyber conflict: where is conflict resolution? In O. Grech (Ed.), *Contemporary issues in conflict resolution* (pp.5-17). Malta: University of Malta. Centre for the Study and Practice of Conflict Resolution, p12; Rouhana, Nadim. N. (2000). Interactive Conflict Resolution: Issues in Theory, Methodology and Evaluation in Paul C. Stern and and Daniel Druckman, *International Conflict Resolution After the Cold War*, National Academy Press, 294-337.

accountable (the EU ECHO Early warning System for example, or the UK's National Cyber Security Centre (NCSC) Early Warning cyber incident notification service). Moreover, and critical to the issue of creating a cyber collective society, it is argued that focusing at the level of region and regional organisations 'born out of the need for building trust and strengthening cooperation among…members…may hold the key to unlocking the stalemate at the global level.'[80] Importantly in relation to the aims of the argument here, this has the potential to move us beyond ineffective discussions on negative peace and stability to positive and sustainable cyber peace through within-region and inter-regional cooperation on issues, for example, such as development, capacity and societal resilience building.[81]

Finally, other scholars have focused on how we might rethink negotiation as part of the interactive conflict resolution toolbox and how we might also reconceptualise conflict resolution practice in the light of the transnational nature of contemporary conflicts, through a cosmopolitan conflict resolution approach.[82] The latter approach is premised on the fact that conflicts are characterised by global-local connectors which include people, capital, networks, weapons etc. and it aims to address drivers of these conflicts in particular, through promoting a value-based approach at the global level. Cyber-attacks and cyber conflict, of course, pose problems for the traditional use of these approaches given issues relating to attribution (i.e. given the need for two sides in any negotiation) and indeed the use of ICTs in conflict, which the field has self-admittedly been slow to react to.[83] To this end, it has been suggested that conflict resolution scholars must think more innovatively on how to engage with relevant agents (hacker/hacktivists) through mediation or negotiation[84] - to secure the various layers in the cyber ecosystem. It has also been suggested that the development of new technologies should be driven by a values-based approach incorporating conflict resolution and peace – through, for example, the training of technical engineers and software developers - and that this in turn should be the basis of any national cyber security policies and strategies as well as those

[80] Pawlak, Patryk., Tick, Emeken., and Kerttunen, Mika (2020), 'Cyber Conflict Uncoded: The EU and conflict prevention in cyberspace', Brief 7, Conflict Series, EU Institute for Security Studies. For other work on preventative diplomacy and cyber see: Kavanagh, Camino and Cornish, Paul, Preventive Diplomacy, ICT and Inter-State Conflict: A Review of Current Practice with Observations," Swiss Federal Department of Foreign Affairs, (forthcoming).
[81] Pawlak et al, Ibid.
[82] Ramsbotham, Oliver., Woodhouse, Tom., and Miall, Hugh., (2016) Contemporary Conflict Resolution (4th ed.), Cambridge: Polity Press, p14.
[83] Gershowitz, Jason and Rule, Colin., (2012) 'Applying Information and Communications Technology to Multiparty Conflict Resolution Processes', *ACResolution,* Fall 2012.
[84] See, for example, Cristal, Moty, 'How to negotiate when hackers are holding you to ransom', *Wired,* 15 May 2017. https://www.wired.co.uk/article/cyber-attacks-hackers-ransoms

of international organisations (and to this we would add regional fora).[85] This would certainly provide a concrete basis for a more nuanced approach to achieving cyber peace, in particular if it is tied to a human-centred narrative and logic, a more complex understanding of cyber violence (and peace) and a practice-based conceptualisation of the cyber ecosystem.

Conclusion

This article has explored the extent to which and more tentatively, how we might (re) consider and *rearticulate* the dominant narrative on cyberwar towards that of cyber peace. We have argued that moving to a positive cyber peace through desecuritisation is desirable and beneficial if we want to create a cyber ecosystem that is sustainable, resilient, rights-based, trustworthy and importantly, where there is an absence of structural violence and the continuous escalation and diffusion of cyber weapons in the name of the national security interest.

Our argument is an ambitious one. Some will ask, if cyber-attacks are an extension of existing, long term and ongoing political and geopolitical disputes, then how can we make progress towards cyber peace? In other words, why is peace possible in cyberspace when it doesn't appear to be in the real world? But this belies the progress has been made in other contested domains – through the emergence of maritime, nuclear, space, oceans and atmosphere regimes, for example. Human-centred approaches to peace, established through activism and social movements, have wrought significant changes in the international system, from the end of apartheid in South Africa to the emergence to the human and civil rights movement and increased awareness and action on climate change. While there are reasons to be sceptical about cyber peace, and different ways to achieve it, there are also harmonies of interest in cyberspace – including the need for the internet to drive international commerce, for example. The nature of the domain is also something that can be managed and improved over time through incentivising more responsible and ethical security practices in the national security, public and private sectors. We are at the beginning of these efforts.

Moving from a vicious to a virtual cycle of positive cyber peace is a desirable, and necessary outcome, if we are to avoid constructing the very vulnerabilities and insecurities that lead to

[85] Wohlfeld and Jasper, op.cit. p13

the prioritisation of offense and destruction, rather than transformative, human-centred development in ICT evolution. For this to happen, several dimensions within the current milieu need to be addressed. First, how we use the language associated with cyber 'attacks' and 'warfare', must be more nuanced and precise among all stakeholders, so that it does not invoke fear and insecurity or indeed reinforce the cyber 'security dilemma' in cyberspace. Second, there must be a reorientation of the way in which the governance of cyberspace is practiced. States will no doubt remain major players in the international cyberspace ecosystem, but a decentralised, layered approach that places peace and rights-based values front and centre of technological development, and which targets issues at source, will prioritise the varied needs of the individual in cyberspace rather than national security interests.

Whilst we consider that there will no doubt be resistance to any rearticulation or indeed silencing of the cyberwar narrative given the vested interests of state and non-state actors in the practices born from these, and that *replacement* is not a viable option, the argument in this article is that *stabilisation* is not enough if we want to avoid the dangers inherent in a negative form of cyber peace. To this end, we suggest there is merit in pursuing *rearticulation* in cyberspace through the tools available in conflict prevention and resolution – mediation, negotiation, preventive diplomacy – in order to begin to reframe the existing cyber narrative and pre-empt future securitization of new technologies, but as important, to replace the prioritisation of the state and national security interests with a human-centred practice that will reduce vulnerabilities, enhance resilience and trust, and ultimately, create a common, collective culture of cybersecurity and a sustainable (positive) cyber peace. This article has offered some preliminary thoughts on where and how this might be done in terms of spaces, agents and levels; thoughts that will need to be developed further in critical conversation with the cyber stakeholder community in terms of the specific conditions through which cyber desecuritisation can be incentivised, as well as the specific processes that could lead to transformative change and the narration and practice of securing cyberspace for the interests of the many, not the few.